



Terms of Use

Definitions

1. Access to Resources
2. Conduct Requirements
3. Use of Resources
4. Acknowledgement and Reporting
5. Termination
6. Provision of Service

Canada's national advanced research computing (ARC) platform is delivered through the Compute Canada Federation (the CCF), which is a partnership of Compute Canada (CC), regional Digital Research Infrastructure (DRI)-serving organizations ([WestGrid](#), [Compute Ontario](#), [Calcul Québec](#) and [ACENET](#)) and academic institutions across Canada. Together, CCF partners provide computing infrastructure and services to a wide variety of academic disciplines from virology to astrophysics and literary analysis.

Definitions

- **Account Holder:** an individual who has a Compute Canada Database (CCDB) account.
- **Compute Canada Federation (CCF):** a partnership of Compute Canada, regional DRI-serving organizations ([WestGrid](#), [Compute Ontario](#), [Calcul Québec](#), and [ACENET](#)), and academic institutions across Canada.

1. Access to Resources

- 1.1 You will never access or attempt to access any CCF resources (or any other user's data on the CCF resources) other than those resources or data to which you have been granted access
- 1.2 You will always abide by any policies, protocols, or requirements that are in effect at institutions with which you are affiliated, such as an Acceptable Use Policy. In a situation in which a conflict exists between the CCF Terms of Use and the policies at institution(s) with which you are affiliated, you must notify¹ the CCF staff and comply with any requirements identified by the CCF staff.
- 1.3 You will not allow any other individual to use your account to access CCF resources. If others require access as part of your research, these individuals must apply for their own account.

¹ Contact by email at support@compute canada.ca or contact your local CCF representative.



- 1.4 Any CCF account credentials and information used for authentication are confidential and you are responsible for keeping them secure.
- 1.5 You will provide and keep up-to-date user information in the Compute Canada Database (CCDB). [Updates can be made by logging into your account at <https://ccdb.computecanada.ca/security/login>].

2. Conduct Requirements

- 2.1 You are responsible for the activities associated with your account and for the use of resources assigned to you.
- 2.2 You are responsible for understanding and meeting any privacy, confidentiality and acceptable use policies, requirements, laws or regulations that apply to your research and data. This includes, for instance, any provincial privacy laws or ethics board requirements affecting any data that you store on CCF systems.
- 2.3 In the event, your account is compromised or suspicious activity is detected related to resources assigned to you, you agree to work with CCF staff and any institution with which you are affiliated to resolve the issue.
- 2.4 At no time will you use CCF resources for any activity that contravenes any applicable laws or regulations. You are responsible for identifying all applicable laws and regulations that may apply.
- 2.5 You agree that should you ever be investigated or found liable for any contravention of Canadian law, or any other applicable laws, the CCF is in no way responsible or liable for such contraventions or for any penalties associated with it. If anyone attempts to make the CCF liable for anything related to your research or your use of CCF resources, you agree to work with CCF staff to address the issue.
- 2.6 You must immediately notify² the CCF if you become aware of any unauthorized access or use of CCF resources or data or of any event that might affect CCF information security or privacy.
- 2.7 You will complete an annual account renewal process to retain access to resources assigned to you.
- 2.8 The CCF reserves the right to define abuse of resources and take appropriate action where and if necessary. For example, it has the right to monitor use of its systems, deactivate an account, or block access to CCF resources.

3. Use of Resources

- 3.1 You will not use the CCF resources in any situation in which failure or fault of the use of the resources could lead to death or serious injury of any person or animal, or serious physical or environmental damage.
- 3.2 You will not introduce software into the CCF environment that may damage, interfere with, or capture any system, program, or data outside of your own

² Contact by email at security@computecanada.ca or contact your local CCF representative.



assigned resources. The CCF reserves the right to identify, quarantine or delete any such software, as well as any related data.

- 3.3 You will not attempt to probe, scan, penetrate or test any CCF services or systems for vulnerability nor to probe, scan, penetrate or test any external services or systems.
- 3.4 You will not try to access or intercept data not intended for yourself or for the resources that are assigned to you.
- 3.5 You will not send or assist with unsolicited bulk communications.
- 3.6 You will not use applications without valid and appropriate licensing.
- 3.7 You will not use software services that would override CCF authentication or policy enforcement.
- 3.8 You will not use software or services that provide unprotected access to shared CCF resources.
- 3.9 You will not knowingly use CCF resources in a manner that impedes or denies the ability of others to use the resources to which they have been granted access.
- 3.10 You are expected to use CCF resources efficiently.

4. Acknowledgement and Reporting

- 4.1 In any publication or communication related to your use of CCF resources, you agree, where possible and appropriate, to acknowledge the CCF's contribution as prescribed in the CCF Acknowledgement Policy.

5. Termination

- 5.1 Failure to abide by these Terms of Use may result in the revocation of access privileges as well as legal action against you or your institution.
- 5.2 If access is revoked or expired, the CCF will archive or retain your data for a one-year period. Temporary data³ will not be preserved and may be deleted at any time. After a year, if no action has been taken to reactivate the account, the CCF reserves the right to permanently delete all of your data.

6. Provision of Service

- 6.1 The CCF reserves the right to move data that is stored in the CCF systems and has been inactive for at least one year to manage and improve overall system performance.
- 6.2 The CCF reserves the right to request documentation that demonstrates that

³ Temporary data includes any information stored on a device not intended for data preservation (e.g. scratch storage, temporary disk allocation, caches, etc.)



proper authorization is in place for the use of CCF resources.

- 6.3 The CCF reserves the right to audit and monitor the usage of, performance, and security posture of its systems to manage service stability, integrity, accessibility, and confidentiality.
- 6.4 To maintain overall system performance, the CCF reserves the right to manage system load. This may include deactivating logins or deleting jobs without notice.