Document version: 1.0
Status: Approved by NAISS Director
Date: 2026-05-27

NAISS General Terms of Use

1. Introduction

NAISS provides HPC, AI, storage, software and support services to users from the public and commercial sectors, with open academic research as the main target. The class of service is defined by the specific access mechanism such as competitive academic research proposals. The legal host organisation of NAISS is Linköping University. The NAISS account and allocation systems might be used to provide access to services provided by other organisations, including local university resources. Unless otherwise specified, the same Terms of Use apply to such services, with NAISS services to be interpreted as services provided by the offering party.

2. Permitted usage

Services can only be used for the purpose for which they have been granted, as specified in a research plan, proposal, contract or other definition. Services may require additional license terms or conditions set by third parties. For example, software or hardware manufacturers or third-party funding authorities may limit the use of services to only open academic research or based on the nationality or affiliation of users. In cases where NAISS requires the user to agree to additional license terms, we will make the terms available to the user in the project portal, or they will be otherwise presented to the user.

Users are responsible for ensuring that their use of the services is in compliance with applicable laws including international law, export restrictions, sanctions and other restrictions, and any applicable regulations and license terms. The user agrees to adhere to the content of the NAISS Export Restrictions and Sanctions available as part of the NAISS policy documents[1].

3. Research results should be public

[1] https://www.naiss.se/policies/export

Unless otherwise agreed, e.g., in a contract for industrial or other commercial use, research results should be published publicly, preferably for peer review. The user commits to follow The European Code of Conduct for Research Integrity.

The user agrees to acknowledge the services provided to produce the results in publications and presentations. Depending on the service and access mechanism, this can be e.g. NAISS, EuroHPC Joint Undertaking, the Knut & Alice Wallenberg Foundation, or another funder. The requested acknowledgment formulations for each service are available at https://www.naiss.se/policies/acknowledge/.

4. Account registration and user access

To use some of the services you must apply for an account. Requirements of user authentication methods, including the accepted identity federations, are described in the NAISS documentation pages. NAISS reserves the right to reject a user application.

Your primary contact information should use an official email address provided by the organisation (e.g. university or company) that you represent and qualifies you for access to NAISS Services e.g. under a call or contract.

NAISS maintains a user register and information sheet in accordance with the General Data Protection Regulation (GDPR) Regulation (EU) 2016/679 and national data protection regulation, and our user portal documentation contains a detailed description of the processing performed.

Users are responsible for keeping contact details up to date at all times, and to monitor their primary email. This will be used to notify users about changes to these terms, service interruptions, service information, and other important issues, including warnings about data deletion after allocation end dates.

NAISS retains the right to monitor and log all usage of, and access to, the services provided to ensure security and verify that the Terms of Use are observed.

NAISS is entitled to publish general information about the user and the purpose for which the user rights have been granted. This includes the user's name, organisation, scientific area, project name, description and resource usage. We may transfer your data outside of the EU/EEA only in connection with services provided by third parties for example to comply with software license agreements, in compliance with Chapter V of the

GDPR on transfer of personal data to third countries or international organisations.

5. Users are responsible for the use of their account and services

NAISS Services include access to powerful systems that can cause major intellectual or economic harm to third parties if abused, and as a user you are responsible for the use of your account.

In particular, you may not:

- Share credentials, leave them unprotected for others to see, or neglect security responsibilities. You should only connect to NAISS services from computer systems that are kept up to date with all security patches.
- Connect remotely to NAISS services from any country subject to export controls or sanctions, not even by going through a server in an approved country.
- Misuse or abuse any NAISS or third-party service or property, including intellectual property such as copyright, or act in violation of any licence terms.
- Interfere with the use of services by other users or compromise the privacy or security of other users.
- Misuse or abuse user content, credentials, or other confidential information.
- Send or transmit harassing, abusive, libellous, obscene, or unsolicited (spam) communications or distribute malicious content.
- Use resources for cryptocurrency mining or storing/processing data unrelated to the approved project.
- Tamper with or deliberately disrupt system resources or network traffic to the services.
- Attempt to breach or circumvent any administrative or security controls.
- Engage in any activity which is illegal under local, national or international law.

Users agree to notify NAISS promptly if their account has been used without permission, if their credentials have been lost or stolen, if they suspect security vulnerabilities, or if they notice any breach to the Terms of Use. Users agree to exercise all reasonable care when accessing services. Users are liable, even after their account has been terminated, for damage and costs to NAISS:

- As a result of violating these Terms of Use.
- As a result of violating third party licensing terms.

Depending on the type of infringement and previous offences, measures taken against a user found to be in breach of the Terms of Use will span from

a reprimand to a permanent withdrawal of access to NAISS services, and where relevant it will be reported to the user's host organisation.

All suspicion of illegal activities, including export control or sanctions violations, will be reported to the relevant authorities for legal enforcement and prosecution.

6. User and project management

Services are allocated as projects. Each Project has a Principal Investigator (PI) user who has the overall responsibility. The PI may designate another user as proxy, which gives the proxy permission to act on behalf of the PI.

- The PI serves as a primary contact person between the project and NAISS.
- The PI can add/remove users to projects, or request NAISS to do so, and is responsible for keeping the list of project members up to date at all times.
- The PI is responsible for ensuring that the identity of each user added to the project is vetted, and that each user fulfils the requirements for access to NAISS services.
- The PI has responsibility for ensuring the project only uses NAISS services for the purpose granted.
- The PI has responsibility for data management of information stored on NAISS resources as part of a project. The PI has rights to access, modify, remove or change ownership of any data belonging to a project (but not personal data in a home directory of a user).
- Upon request, e.g. when specified for an allocation, the PI must submit a report on the progress of the project and the use of the services.

A project is valid for the time communicated in connection with the allocation. NAISS will notify project members before the expiration date upon which the users' accounts may be terminated. Projects are encouraged to use resources in a balanced way during their whole project lifecycle and start to use the resource early in the project lifetime. If certain resources have not been used by milestones defined for each Service, the unused resources might be cut to the limits detailed in the corresponding allocation or cut-off policy.

7. Automated or Headless Usage

For certain services, NAISS might offer support for employing automated tools, scripts, workflow systems, orchestration frameworks, CI/CD services, AI agents, or other non-interactive mechanisms to access resources, provided that:

- Such usage is explicitly authorized for the allocation, access scheme, and resource in question, and the user does not try to hide automated usage.
- Automated access is performed using approved authentication mechanisms.
- Credentials are handled securely and may not be embedded in publicly accessible code, containers, repositories, or workflows.
- Automated systems operate under the responsibility of an identifiable authorized user and project.
- The responsible user remains accountable for all actions performed by automated systems acting on their behalf.
- Automated usage must not circumvent allocation limits, security controls, accounting systems, audit mechanisms, or usage policies.
- Users must ensure that automated systems do not create excessive, uncontrolled, or harmful load on infrastructure services.
- At any time, NAISS may without notice limit, suspend, or revoke automated access mechanisms that negatively impact system stability, security, fairness, or other users.

8. User content

User content includes the user's data, software, servers, systems, or processes that use or interact with the services. The user is responsible for content stored in, or transmitted via, NAISS services and that it complies with applicable laws and regulations, data policies, and with the provisions included in these terms.

The user gives NAISS the right to access content to secure accessibility, quality and security. This includes keeping the information on the NAISS service platforms, automated monitoring for intrusion detection, taking backups, copying/moving content, or reproducing faults. NAISS protects the confidentiality of content as permitted by law. For sensitive data, NAISS will restrict access to staff with explicit permission, and all access will be logged.

NAISS provides an IT service platform that enable users to independently process their content. Access to NAISS resources does not entail transfer of custody or administrative responsibility for user content to NAISS or Linköping University.

Users are responsible for sharing of their content according to the project's and their own requirements. For example, if a user leaves a project, they should ensure they transfer project content to another user of that project. All user content in storage connected to expired projects will be deleted after a waiting period of 90 days.

Upon request, NAISS will make a reasonable effort to provide the user with a copy of content to which the user has ownership or intellectual property rights after account cancellation or termination. The user must make such requests within 90 days of cancellation or termination and provide NAISS with a location

to store the copy of content. Copies of content may technically remain on Backup Storage, but access to the data will be strictly restricted.

9. Processing sensitive data in user content

If Content contains special categories of personal data (i.e., sensitive data), referring to the GDPR articles 4(1) and 9(1), or any other type of confidential data, the user has to ensure that the service intended to process the data complies with the security level required for this kind of data.

Sensitive data can only be processed with services explicitly specified for such purposes, and where the user's organisation has signed a Personal Data Processing Agreement with the organisation providing the service (typically Linköping University).

In such a case, the main responsibility for the data remains with the user's organisation, and the user commits to take care of the data controller's responsibilities as described in applicable data protection legislation. NAISS acts as a processor of the personal data. The user and NAISS will execute the data processing agreement and will execute the description of processing activities which together govern such processing activities.

NAISS offers an IT service platform according to the service descriptions and these Terms of Use for the users to process their content on their own account. NAISS implements and maintains the measures required by the security of the processing according to the service descriptions and the certified security system.

10. Backups are limited and not guaranteed

NAISS might make backup copies of some content to reduce the risk of data loss for common issues. This is defined in the relevant service description. However, backups are not always technically feasible for all content, e.g. for performance reasons, and even when backups are made it is theoretically possible for backups to fail. NAISS provides no guarantee for restoring any content and declines any liability for lost files or data for any reason. Users who have content they cannot afford to lose should maintain at least one up-to-date copy on other media.

11. Service level declaration and limited warranty

Use of the services is at the user's own risk, and NAISS is not liable for any loss or injury, including loss or injury caused by possible erroneous results. NAISS does not provide any warranty or representation as to the availability, error- or interruption-free operation, or suitability for any purposes (general or particular) of the services, or any warranty that

communications to or from the service is completely secure. NAISS expressly disclaims any express or implied warranties.

However, NAISS aims to follow industry best practice service management and security measures. NAISS reserves the right to modify and terminate any service at any time. NAISS may from time to time make changes to any interfaces made available to the service. We aim to provide advance notice of such changes, but this might not always be possible, e.g. for security reasons.

12. Termination of User Accounts

The NAISS account is valid for a fixed time period, starting from the day when the account is opened. NAISS will notify users well before the expiration date of the account.

The right to use NAISS services ends when the original purpose is no longer valid or the user has parted from their affiliated organisation. The PI of the project makes the decision whether the user can continue the use of Services when affiliated to a new organisation. If the User is the PI of the project, they must contact the party who has made the allocation decision for the project in order to verify their eligibility.

The user account and associated content will be handled according to the corresponding service descriptions and their terms of use. NAISS will notify the user about their expired account via the contact information provided by the user before deleting user content and account.

The user account can be terminated or suspended by NAISS without notice:

- In the event of any unauthorized use of the services.
- If NAISS has a justified reason to suspect that the services are used contrary to these Terms.

You can terminate your user account by giving notice to the NAISS support. NAISS will retain and use general user information as described in these Terms to fulfil our reporting and statistics requirements. All such historical data will be erased after at most 10 years according to data retention policies defined by Swedish law.

13. Resource Allocation cut-off policies

For certain services allocated with a fixed total quota, NAISS might use the EuroHPC JU policy to apply a cut-off policy for their resource allocation if projects do not consume their allocated resources early enough. NAISS provides a copy of the policy in place for each service and/or allocation as part of our documentation.

For resource allocations that might be subject to a cut-off, NAISS will notify the project Principal Investigator at least one month in advance to provide early information and opportunities to react and further plan on both the user and resource allocator’s side.

14. Fair-share scheduling

For certain services allocated with monthly quotas, NAISS might use fair-share scheduling. The fair-share scheduling means that projects and users

who have used less than their quota the last few weeks will get higher queue priority while ones above their quota will get lower priority. This makes it possible for users to get high throughput in periods where the system has low utilisation, and sometimes even use more than their total allocation. However, projects where one or more users have high recent usage will be subject to reduced priority for all users in the project.

15. Changes to these Terms & Implied User Acceptance

NAISS reserves the right to change these Terms from time to time by notifying the user at least two weeks in advance of the amendment becoming effective. If the user continues to use the services after the stated effective date of the amended Terms, the user is deemed to have accepted the amendment.

16. General

These Terms are governed by Swedish law. The Linköping Administrative Court will have exclusive jurisdiction to deal with any dispute which may arise out of or in connection with these Terms or the User's use of the services, unless otherwise has been agreed.