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

NAISS Export Control and Sanctions

1. Limitations on usage

NAISS operates computational infrastructure within a regulatory framework where services are restricted due to (i) EU & Swedish dual-use regulations for technology that can have both civilian and military applications, (ii) EU & Swedish political sanctions, and (iii) contractual agreements with vendors delivering hardware and software that require NAISS to adhere in particular to US export restrictions and sanctions.

This document defines NAISS requirements, user obligations towards NAISS, and it provides general information, but it does not constitute legal advice. Users are recommended to consult their legal division for advice on specific cases.

2. EU & Swedish restrictions on dual-use technology

The NAISS hardware and system specifications, software, technical data, models, workflows, or research results processed or generated using NAISS services may in some circumstances be subject to export control or dual-use restrictions subject to EU Dual-Use regulation 2021/821[1] that is also implemented in Swedish law[2]. Such items and information cannot be exported outside the EU without permission, with exception for certain countries listed in the regulation (currently e.g. Australia, Iceland, Japan, Canada, Liechtenstein, New Zealand, Norway, Switzerland, the United Kingdom and the United States). Certain other countries also have more specific exceptions; consult the regulation for up-to-date information.

Annex I of the regulation contains an extensive list of technologies where export authorisation is often required. In the context of typical NAISS usage, this particularly includes several items in nuclear and materials science, electronics, computer systems, telecommunications and “information security”, as well as aerospace and propulsion technology. Access to NAISS

[1] http://data.europa.eu/eli/reg/2021/821/
[2] ”Lag (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd” and ordinance “Förordning (2000:1217) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd.”

services may fall under these restrictions and as an operational policy, it is therefore only allowed when users are present in the EU or the countries above.

To share data or results from research, users should consult the legal staff at their institution to assess whether this falls under dual-use restrictions.

3. Restrictions due to EU & Swedish sanctions

NAISS services are subject to sanctions put in place by the EU, as described in the EU sanctions & related resources overview[3], where you can also find up-to-date sanction maps[4] of relevant countries with information about the specific regulations in place for each country. This includes remote access or export of results to sanctioned countries as well as access for individuals on a sanction list themselves or affiliated with a sanctioned organisation or entity, including research institutions in some sanctioned countries. Swedish sanctions are typically fully aligned with the EU and UN, and the Swedish Foreign ministry provides a summary of current sanctions[5].

As of May 2026, there are comprehensive EU sanctions covering Russia, Belarus, Iran, Syria, North Korea, and the Crimea, Donetsk and Luhansk occupied Ukrainian territories. In total there are some 40 sanctions in place targeting either countries, geographical regions, organisations or themes. Users should consult the latest available information.

4. Restrictions due to US export control & sanctions

To deliver infrastructure services, NAISS is dependent on hardware and software from the US, and as part of the purchase contracts the hardware, software, and services used by NAISS are subject to contractual and regulatory obligations related to U.S. export control and sanctions regulations. The US International Trade Administration provides a summary of current legislation[6], and a detailed list of countries and technologies is available in the U.S. Export Administration Regulations (EAR), specifically the Commerce Control List and Country Chart (15 CFR Part 738)[7].

Export control restrictions may also apply to AI models, training data, model

[3] https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/overview-sanctions-and-related-resources_en
[4] https://www.sanctionsmap.eu
[5] https://www.government.se/government-policy/foreign-and-security-policy/international-sanctions/
[6] https://www.trade.gov/us-export-controls
[7] https://www.bis.gov/regulations/ear/738#supplement-1-738

weights, inference services, fine-tuning workflows, and related computational services.

As of May 2026, US export control and sanctions regulations impose significant restrictions, licensing requirements, or embargoes affecting a number of countries, including but not limited to China, Cuba, Iran, North Korea, Russia, Syria, Belarus, and certain occupied territories. Users should consult the latest available information.

5. User obligations

The usage restrictions in the areas above are typically based on individual actions, organisational affiliation or the current geographical location of the user rather than citizenship. When applying for a NAISS project, adding members, or creating a user account, you confirm:

- Your use of NAISS services or the results generated using NAISS services do not violate any export control regulations or sanctions.
- You are not on any sanctions list. The PI of a project should take reasonable steps to ensure that no project member is on a sanctions list.
- You do not have any commitments that would violate export control or sanctions legislation.
- You are not affiliated with organizations subject to applicable sanctions or export restrictions.
- You will not attempt to access NAISS systems, either directly or through proxy systems, VPNs, intermediaries, or other technical means, when physically present in a territory subject to export control or sanctions.
- You will not transfer content, for example software, computing results, research data, AI models, model weights, or resulting knowledge, to countries, organisations, or entities subject to export restrictions or sanctions. Such transfers may include cloud services, external storage platforms, collaborative repositories, and third-party computational environments.
- You will follow all export restrictions by the software vendor of the software you are using.
- You will not circumvent the above-mentioned prohibitions by technical means.

If you are uncertain whether export restrictions or sanctions apply to your research project, we recommend asking your organisation’s legal division for advice or contacting NAISS support.

6. Enforcement

NAISS may perform sanctions and compliance screening of users, affiliations, organisations, projects, and access locations, and reserves the

right to suspend or terminate access without prior notice where necessary for compliance or security reasons.

Users, PIs, resource allocators, and administrators are required to notify NAISS of suspected violations of export control regulations, sanctions, contractual restrictions, security requirements, or other unlawful activities related to NAISS services.

If NAISS has reasons to suspect that services are used partially or entirely against export restrictions or sanctions, it may be reported to one or more of the Swedish Inspectorate of Strategic Products (ISP), the Swedish Police Authority, the Swedish Security Service (Säkerhetspolisen), and other competent national authorities in Sweden or the user's home country. The user's home organisation as well as resource allocator may also be notified. Information required to investigate suspected violations may be shared with these institutions.

Users need to be aware that unlawful export, transfer, disclosure, or use of controlled technology, software, technical data, or computational resources may constitute serious criminal offences. Convictions under applicable export control, sanctions, or security legislation may carry substantial penalties, including multi-year terms of imprisonment.