



Usage Policy for the Computing Infrastructure of the Center for Scientific Computing of UNESP

■ Important

By creating a GridUnesp account, you automatically agree to the terms of this policy. Read it carefully before using the resources.

Preamble

Computing is a tool increasingly used by Unesp researchers in the development of their scientific projects. When used inappropriately, it can cause large-scale problems, affecting the operations and security not only of the institution but of the entire global computing infrastructure.

This policy establishes general rules and procedures of conduct for the proper use of the computing infrastructure of the Center for Scientific Computing of Unesp (NCC/Unesp).

Objectives

This policy aims to:

1. **Ensure a computing environment** that is friendly, productive, and reliable
2. **Maintain an environment that supports global collaboration**, enabling innovation and the free exchange of scientific information
3. **Protect the reputation of the NCC** and safeguard its systems and data against external attacks and unauthorized use
4. **Ensure compliance** with all applicable legal guidelines

User Responsibilities

Account and Access

- Your account is **personal and non-transferable**
- You are responsible for choosing **secure passwords** and keeping them confidential
- Sharing passwords with third parties is **expressly prohibited**
- You are responsible for all activities carried out with your account
- If you suspect your account has been compromised, the password must be changed **immediately**

■ Never share your password with anyone, including:

- Project colleagues
- Advisors or coordinators
- Members of the GridUnesp team (who will never ask for your password)



Acceptable Use of Resources

The NCC computing resources must be used **solely and exclusively** to run tasks related to **previously registered scientific projects**.

Permitted uses:

- Processing of scientific data
- Computational simulations
- Analysis of experimental data
- Development of code for research
- Temporary storage of research data

Fair Use

The user commits to using only the resources necessary for their scientific activity, avoiding waste. This includes:

- Requesting only the amount of resources (CPU, memory, time, storage) strictly necessary for the execution of the work
- Not using resources in quantities greater than what would be reasonably expected for the task at hand
- Optimizing jobs for efficient resource usage
- Contributing to the equitable sharing of the infrastructure

Prohibited Activities

The use of GridUnesp resources is **expressly prohibited** for:

1. Illegal activities of any kind:

- Copyright infringement
- Unauthorized access to systems
- Distribution of illegal content

2. Activities that are offensive or cause public embarrassment:

- Hate speech
- Harassment or defamation
- Offensive content

3. Activities involving personal financial gain:

- Cryptocurrency mining or equivalent activities
- Commercial services
- Hosting of commercial websites
- Training or inference of artificial intelligence models that are inconsistent with the scientific objectives of the registered project or that unjustifiably compromise shared resources

4. Download, upload, or storage of sexual material:

- Pornography
- Adult content unrelated to research

5. Running tasks that use an amount of resources incompatible with resource sharing:



- Intentional monopolization of resources
- Jobs that degrade the overall performance of the system
- Stress testing
- Continuous benchmarking
- Internal denial of service

6. Running tasks that result in software license violations:

- Unlicensed use of commercial software
- Unauthorized distribution of proprietary software

7. Distribution or storage of copyrighted material without a license:

- Music, movies, commercial software

■ Violating these rules may result in:

- Immediate account suspension
- Permanent cancellation of access
- Reporting to the competent authorities
- Civil and criminal liability

Citation Policy

Every user of the computing infrastructure provided by the Center for Scientific Computing of Unesp commits to:

- 1. Include an acknowledgment in publications** — In all articles submitted to scientific journals, conference proceedings, theses, dissertations, and other academic works that use GridUnesp computing resources, the following acknowledgment must appear:

For publications in English:

"This research was supported by resources supplied by the Center for Scientific Computing (NCC/GridUNESP) of the São Paulo State University (UNESP)."

For publications in Portuguese:

"Esta pesquisa tornou-se possível graças aos recursos computacionais disponibilizados pelo Núcleo de Computação Científica (NCC/GridUNESP) da Universidade Estadual Paulista (UNESP)."

- 2. Report publications to the NCC** — Send the NCC a copy of the publication (or a link to access it) so that it can be included on the NCC page and be part of the Center's annual activity report.

E-mail for submission: support.ncc@unesp.br



■ Reporting publications is essential to:

- Justify investments in computing infrastructure
- Obtain funding for upgrades and maintenance
- Demonstrate the impact of GridUnesp on scientific output
- Strengthen Unesp's position in the HPC landscape

Backup and Data Responsibility

Backup Policy

GridUnesp does NOT perform automatic backups of user data.

Exceptions: upon formal request by the project coordinator; express authorization from the NCC management; specific cases agreed in advance.

User responsibility:

- Keep backup copies of important data
- Transfer critical results to your own systems
- Do not use the cluster as your only storage location
- Preserve data needed for research reproducibility

■ In case of a catastrophic failure of the storage system:

- **Data will be lost with no possibility of recovery**
- The NCC is not responsible for data loss

Recommendations:

1. Keep at least **two copies** of important data
2. Use **version control** (git) for scripts and code
3. Transfer results to your local computer **regularly**
4. Consider institutional repositories for long-term data
5. **Data stored on the infrastructure should not be considered primary or permanent copies**

Data Protection (LGPD)

GridUnesp follows the guidelines of the **General Data Protection Law (LGPD) — Law No. 13,709/2018** regarding users' personal data.

Principles applied:

- **Purpose:** The collected data is used exclusively for access management and cluster operation
- **Transparency:** Users are informed about which data is collected and how it is used
- **Security:** Technical and administrative measures are adopted to protect data against unauthorized access



- **Access and correction:** Users may request access to, correction of, or deletion of their personal data

Data collected:

- Name, e-mail, and institutional affiliation: for contacting and supporting users
- Login (username) and password hash (stored securely): for access to the GridUnesp account
- Access and cluster usage logs: for operational and security purposes

User rights:

- Request confirmation that data processing exists
- Access the personal data held by the NCC
- Request correction of incomplete, inaccurate, or outdated data
- Request anonymization, blocking, or deletion of unnecessary data

Projects that use personal or sensitive data must fully comply with the General Data Protection Law (Law No. 13,709/2018), and it is the responsibility of the principal investigator to ensure compliance.

Channel for requests related to personal data:

- E-mail: support.ncc@unesp.br (subject: "LGPD")

Software Responsibility

User-installed software

The user is responsible for the content of applications, libraries, or containers installed under their responsibility, as well as for ensuring that such software does not compromise the security or stability of the system.

Software security

The user should keep software under their responsibility updated whenever possible, applying security patches when available.

Commercial software and licenses

The use of commercial software on the GridUnesp infrastructure must fully comply with the licensing terms of each product, and it is the user's responsibility to obtain and maintain the necessary licenses.

Cooperation

The user shall cooperate with the technical team in the investigation of security incidents or operational problems. This includes:

- Providing accurate and complete information about suspicious activities
- Responding promptly to inquiries from the technical team
- Allowing access to relevant logs and data for investigation, when requested
- Following guidance provided by the technical team for problem resolution



Obligation to Report Incidents

Every user is required to immediately report any suspected violation of the security rules.

What to report:

- Unauthorized access to your account
- Suspicious activity in your directories
- Jobs you did not submit
- Identified vulnerabilities
- Anomalous system behavior

How to report:

- E-mail: `support.ncc@unesp.br` (subject: "SECURITY INCIDENT")

Required information:

- Detailed description of the incident
- Approximate date and time
- Available evidence (logs, messages)
- Your username and contact

Confidentiality

Disclosing information about security incidents without prior authorization from the NCC is prohibited.

This includes:

- Posts on social media
- Discussions in public forums
- Sharing with unauthorized people
- Academic publications without authorization

Privacy and Monitoring

Privacy Policy

The NCC protects the privacy of all users, in accordance with the LGPD. No inspection or examination of your files will be performed without:

- Your **explicit authorization**
- **Authorization from the NCC Scientific Director**

Exceptions (without prior authorization):

- Situations involving a **compromise of system security**
- Well-founded suspicion of **misuse of resources**
- A **court order** (duly justified)



In these cases:

- Access will be carried out in a controlled manner
- The user will be notified (when possible)

Activity Monitoring

The NCC continuously monitors:

- System performance
- Resource usage per user
- Attempts to access the cluster
- Suspicious activity

This monitoring aims to:

- Ensure system stability
- Identify technical problems
- Prevent improper use
- Collect usage statistics

Sanctions and Penalties

Failure to comply with this policy may result in:

Warnings (minor violations):

- Notification by e-mail
- Guidance on correct use

Temporary suspension (moderate violations):

- Account blocked for a defined period
- Notification of the project coordinator
- A corrective action plan required

Permanent cancellation (serious violations):

- Immediate account removal
- Prohibition of re-registration
- Reporting to the competent authorities
- Formal notification to the originating unit

Serious violations include:

- Attacks on systems
- Password sharing
- Commercial use of resources
- Illegal activities
- Repeat moderate violations



■ Note

The NCC team reserves the right to immediately suspend any account that poses a risk to the security or stability of the system, without prior notice.

Failure to comply with this policy may result in temporary or permanent suspension of access to the computing resources, without prejudice to any other applicable administrative and legal measures.

Final Provisions

Validity

This policy takes effect on its publication date and applies to all current and future GridUnesp users.

Policy Updates

This policy may be updated periodically to reflect technological, legal, or operational changes. Updates will be communicated to users with reasonable advance notice:

- By e-mail to registered users
- On the official GridUnesp page
- In the user documentation

Acceptance

Continued use of the infrastructure implies agreement with this policy and any future updates.

Questions and Clarifications

Questions about the appropriate use of the computing resources should be directed to:

Support team of the Center for Scientific Computing

- E-mail: support.ncc@unesp.br

Statement of Awareness

By creating a GridUnesp account, the user declares that they:

1. Have read and fully understood this policy
2. Commit to complying with it in full
3. Take responsibility for all activities carried out with their account
4. Agree to the sanctions provided in case of non-compliance