

Regulations complement ICT CSIC policies and regulations and are intended to establish the necessary provisions to maintain the security and integrity of IAA communications networks and computer services.

1. User support and computer equipment

- Computer Center only can provide support to IAA staff and to computer equipment registered in the IAA inventory.
- User account management is handled by [Human Resources](#) staff.
- Issues must be reported through [Request Tracker](#). Before register an issue, check Computer Center [website](#).
- Computer Center does not have computer equipment or accessories to provide to users.
- Contact [Purchasing Department](#) for any question about computer equipment request, procedures for acquisition, warranty and repair.
- All computer equipment that require support for installation, administration, management or maintenance, must be approved by the Computer Center.
- Research groups that have computer equipment to implement their own services, must have IAA staff assigned to its installation, administration, management and maintenance.
- Users are liable for the access and use of computer resources. Computer Center never be liable in any way for the integrity, content, use or publication of information stored on user computer equipment.
- Users are liable for make and keep their backups.
- Computer Center will suspend any harmful activity for IAA computer services integrity or performance.

2. Communications networks

- User credentials that identify the access to communications networks, are personal and non-transferable, and the user is the only liable of them.
- Communications networks will be exclusively used in order to carry out IAA activities, being their use expressly forbidden for any illegal practice or with profit making objectives.
- Forbidden send spam, transmit fraudulent, defamatory, offensive, vandalistic or harassment content, and spread malware, computer viruses or similar.
- Forbidden obtain, manipulate or share any file without having intellectual property rights on it. It is also forbidden intercept, compile or storage third party data without their knowledge and consent.
- Forbidden, both inside and outside communications networks, scan or test the vulnerability of equipment, systems or devices. It is also forbidden to gain unauthorized access to them.
- Communications networks must be used secure and efficiently, avoiding practices that might cause congestion or compromise their security, such as the use of techniques or devices for creating or configuring other networks.
- Computer Center cannot guarantee the privacy and safety of user data when using communications networks. Neither can guarantee the availability and quality of communications services, and will may establish usage limits or suspend services in order to protect communications networks from fraud or activities that not complying the current legislation.

3. Consent

- User declare that have read, understood and agree the terms of use, when access and use IAA computer services and communications networks. Non compliance of such terms may lead in revocation of use rights, including legal sanctions if applicable.

4. Computer equipment housing in computer rooms

- Housing may be provided if there are available resources to meet equipment requirements of space, cooling and power supply.
- Equipment must be in rack format and can only be housed in 19-inch rack cabinets. It must be approved and supported by the manufacturer, and must be removed when becomes obsolete.
- Equipment must belong to a research project and have IAA staff assigned to its installation, administration, management and maintenance.
- Equipment will be managed remotely. Computer Center must authorize access to the computer rooms and reserves the right to change equipment physical location.

Granada, October 1, 2025

