Acceptable Use Policy for ReCaS-Bari Computing Resources

The Acceptable Use Policy for ReCaS-Bari Computing Resources are:

Network Acceptable Use Policy - AUP

1. The Italian University and Scientific Research Network, which is commonly known as "the GARR Network" is based upon projects involving scientific and academic cooperation among Universities, Schools, and Public Research Institutions in Italy. GARR network service and the other related services are therefore principally intended for communities which are supervised by the Ministry of Education, Universities, and Research (in brief, the MIUR). There shall also be the possibility of extending the aforementioned service to other contexts, such as institutions which are supervised by other Ministries which may have adopted a specific Contract with the Consortium GARR, or institutions where research activity is being pursued in Italy, specifically but not solely in the instance of "non-profit" institutions which are participating in cooperation with the community supervised by the MIUR. Use of the Network and its services shall depend, in all instances, upon compliance with Acceptable Use Policies (AUP's) by all GARR users.
2. "GARR Network Service", which is briefly defined hereinafter as the "GARR Network", consists of the entirety of data transmission services, network management services, application services, storage and computing services and of all the interoperability tools (which are to be provided directly by the Consortium GARR or on its behalf) allowing authorized subjects to communicate with one another (National GARR Network). Data transmission and services allowing interconnections between the national GARR Network and other networks are an integral part of the GARR Network.
3. The following activities are not permitted within the GARR Network:
    - providing unauthorized parties with access to the GARR Network, network connectivity services, or other services which may involve it, such as providing housing and hosting services and similar services, as well as allowing routing of data and/or information on the GARR Network between two parties for whom access to the GARR Network shall not be allowed (Third party routing);
    - using network, storage or computing services or resources, connecting hardware or services or software to the network, disseminating viruses, hoaxes, or other programs in such a manner that the activities of other persons, users, or services which are available within the GARR Network or other networks which are connected to it, may be harmed, hindered, or disrupted;
    - creating or transmitting or store (unless these activities may occur for research purposes or in a specifically regulated and lawful mode in all instances) any images, data, or other material, which may be offensive,

libelous, obscene, or indecent, or which may offend human dignity, specially if said items pertain to gender, race, or religious beliefs;
    - transmitting unrequested commercial and/or advertising material ("spamming"), as well as allowing the use of one's own resources by third parties for activities of this kind;
    - damaging, destroying, or seeking unauthorized access to data, or violating other users' confidentiality, including interception or dissemination of passwords, confidential cryptographic codes, and any other personal data, as it is defined by legislation pertaining to privacy protection;
    - engaging in any other activities on the GARR Network which may be prohibited by the domestic legislation, by international standards, or by rules and customs ("netiquette") pertaining the use of networks and the access to network services;
4. Responsibility for the content of materials being produced and disseminated using the network and its services is attributable to the persons producing and disseminating said materials. In situations involving persons who have not attained adulthood, responsibility may also involve persons whom the law defines as guardians in relation to minors' activities.
5. Participants who are allowed access (S.A.) to GARR Network, as defined by the document "GARR Network Access Rules", may use the Network and its services for all of their own institutional activities. Institutional activities are to be understood as any activity pertaining to completion of functions defined by the statute of an authorized participant, including activities within the context of contracts or agreements which have been approved by the respective probated institutions, provided that use shall occur for institutional purposes. Institutional activities shall specifically include participants' research and educational activities, administrative functions and functions involving participants for whom access is allowed, along with research activities on behalf of third parties, with exclusion of any situations which are explicitly not allowed by this document.
   Other participants who are approved for temporary network access (S.A.T.) may only engage in the entire series of activities indicated within the authorization itself.
   Final decisions concerning the permissibility of a given activity within the GARR Network shall continue to be a prerogative of the Consortium GARR management bodies.
6. All users to whom access to the GARR Network and its services shall be provided must be recognized and identifiable. Hence, all necessary measures for preventing access by unidentified users must be adopted. Normally, users must be employees of participants who may be authorized, even on a temporary basis, to access the GARR Network.
   As far as subjects who are authorized (S.A.) for access to the GARR Network are concerned, users may also be individuals who shall have received temporary permission from the aforementioned participants as a result of employment relationships for institutional purposes. Students who are regularly enrolled in courses at an authorized entity with access to the GARR Network shall be permissible users.
7. Entities which are authorized to obtain access to the GARR Network, even on a

temporary basis, shall be responsible to the GARR Network for adopting all reasonable measures for ensuring consistency between their own rules and those which have been presented herein, as well as for ensuring that forms of use which are not allowed by the GARR Network shall not occur. Each entity with access to the GARR Network must also provide its own users with knowledge (by methods which may be deemed appropriate) of the rules contained within this document.

8. Entities which are authorized to obtain access to the GARR Network and its services, even on a temporary basis, explicitly agree that their identifying information (name of institution, company name, or equivalent information) shall be included in an electronic yearbook which shall be maintained under the responsibility of the GARR Consortium's management bodies.
9. In the event of demonstrated noncompliance with these rules for the use of the Network and its services, the Consortium GARR management bodies shall adopt appropriate measures which may be necessary for restoring the proper functionality of the network, including temporary or definitive suspension of access to the GARR Network *per se*.
10. Access to the GARR Network and its services shall depend upon complete acceptance of rules contained within this document.

Additional rules

The following activities are prohibited:

- activities that contravene the national and international law, in breach of Community legislation or are not permitted by the ordinary usage of the networks and the services provided.
- unauthorized commercial activities, or any other profit-making activities. The transmission of commercial and/or spamming advertising material, as well as the use of its resources by third parties for such activities.
- activities liable to damage, destroy, jeopardize the security of INFN IT resources, or aimed at breaking the privacy and/or at damaging third parties, including the creation, transmission and preservation of images, data or any other material that is offensive, obscene, defamatory, indecent or likely to undermine human dignity, especially when relevant to sex, race, religion, political opinions or personal and social condition.
- activities in conflict with other institutional aims.

The use of IT resources for personal aims may be tolerated as long as it does not violate any applicable laws and complies with the rules of this regulation and with all the provided indications.

Users shall:

1. act in compliance with the law and in accordance with the security directions provided by Computing and Networking Service. They are required to ensure the privacy of processed personal data by proper observance of the rules available at the following web page: www.infn.it/privacy/;
2. take into account the guidelines provided by the Computing and Networking Service concerning the selection of computing devices to use, especially if they concern security-related features. They shall prefer systems and procedures that offer the

highest levels of protection;

3. be responsible for the data and for the software they install on the computers entrusted to them: they are required to examine software carefully and in advance and do not install any software with no regular licenses;
4. regularly update the software installed on the computers entrusted to them;
5. protect from unauthorized access data used and/or stored in the computers and systems they are allowed to access;
6. carefully evaluate the reliability of external services, including cloud services, in terms of security, storage and data confidentiality.
7. follow the Computing and Networking Service recommendations concerning the regular backup of data and used programmes;
8. protect their account avoiding to choose obvious passwords and in the event of multiple authentication systems by using different passwords for each system.
9. not share their passwords, nor allow even occasional use by anyone other than the account holder;
10. immediately notify any incidents, suspected abuses and security breaches to their contact person and to the Computing and Networking Service.
11. use updated anti-virus software where operating systems require that. They shall take care to scan all software and files exchanged over the network and all removable media they use;
12. not maintain unused remote connections nor leave their workstation unattended with unprotected open connections.