INFN–CNAF Acceptable Use Policy (AUP)

This document describes the general security rules for access and use of INFN-CNAF Computing and Network resources. The official electronic version of this document is available at this URL: http://www.cnaf.infn.it/policy/AUP-CNAF-EN.pdf

All users of INFN-CNAF resources must read and accept everything written in this document and must strictly adhere to this AUP. Any action not compliant with this AUP will be considered a “Security violation” and will imply the revocation of authorization to access INFN-CNAF computing and network resources. In serious cases, the violation may be reported to competent legal authorities.

Utilization rules for INFN-CNAF computing and networking resources

INFN-CNAF computing and network resources are dedicated to scientific and technological research and may be used exclusively for institutional INFN activities.

1. All users, to whom access to internal computing or network resources is granted, must be clearly identifiable.

2. The personal access credentials are strictly personal, and can’t be shared or given to anyone.

3. The connection of any device to the INFN-CNAF network must be explicitly authorized by the INFN-CNAF Network Division.

4. The installation of any network service (for example: DNS, DHCP, Mail, http, https, ssh, etc..) must be explicitly authorized by the INFN-CNAF Network Division.

5. The responsibility for the contents published on the INFN-CNAF network rests with the producer or owner of the information.
6. All the following activities are strictly forbidden:

a. To give access to INFN-CNAF internal computing or networking resources to anyone not expressly authorized.

b. To log in or access resources using false credentials or credential of other users.

c. To install, run, or distribute software (including, but not limited to, Viruses, Worms, Trojans, Hacking tools, etc.) that could damage or degrade INFN-CNAF computing and network resources, or resources of other sites.

d. To damage, destroy or attempt to access other users’ data without authorization, or to violate other users’ privacy.

e. To create or send (if not for research purposes, to be performed in any case in an authorized, controlled, and legal way) any kind of image, data or other offensive item, libel or indecent document that offends human's dignity, in particular with regards to sex, race or faith.

f. Any activity that could violate current informatics and communication technology laws.

g. Any copyright violation activity.

h. Any activity that could compromise in any way the security of INFN CNAF or of third-party resources.

i. Any commercial activity not explicitly authorized by INFN.

j. In general, all illegal activities.

7. Any suspicious or malicious activity, or any incident or security violation, is to be reported immediately to the INFN CNAF Network division.