Allegato n. 4

CONDITIONS OF USE FOR INFN'S COMPUTING RESOURCES

Use of computing resources and network services

The computing resources and and network services of INFN represent very important resources that INFN makes available exclusively to achieve its institutional scientific and technological research goals. The cooperation of those authorised to use them is essential for preserving their integrity and for guaranteeing their performance.

The following is forbidden:

- Activities contrary to the law or prohibited by regulations;
- Unauthorized commercial activities;
- Any activity which compromises the security of the data resources of the Organisation or intended to cause damage to third parties;
- Any activity not related to the goals of the Organisation.

Access to data resources and network services

Access to the data resources and network services of INFN is permitted to employees, associates, as well as partners, guests, research students, undergraduate students, PhD students and grant holders authorised by their supervisors.

Access to the computing resources that provides Internet connection is allowed only through user identification. Users who have not been formally identified as a consequence of their position as INFN employees, or affiliated to INFN as holder of associates status, INFN research grant or post-doc contract, are identified by presenting a copy of a document of identity and registration of date reported therein.

Access is personal, cannot be shared or passed on and is permitted to each user solely in respect of the provisions of these regulations. Providing access to a third party is forbidden without prior authorisation from the local Computing Service.

In order to guarantee the security of the data resources, the following is forbidden:

- Unauthorised access to the computing rooms, as well as to reserved places and areas where network equipment is located;
- To connect computing resources to the local network without proper authorisation from the local INFN Computing and Network Service;
- To wire, connect or modify network apparatus without the relevant authorisation from the local INFN Computing and Network Service;
- To use network addresses and names other than those explicitly assigned to the user;
- To install modems configured for remote access without preventive authorisation from the Director of center;
- To divulge information about the structure and configuration of IT resources, particularly for what

concerns the location of wireless equipment, telephone numbers and the passwords of modems managed by the local INFN Computing and Network Service;

- To undertake any other direct action intended to degrade the system's resources, to prevent authorised users from accessing resources, to obtain superior resources to those already allocated and authorised, to access the data resources in violation of security measures.

Behavioural rules for users

Users:

- Are bound to act in conformity with the law and in respect of the policies of the Organisation on subjects of security, guaranteeing the confidentiality of the treatment of personal data, also through the strict observance of the rules of conduct laid down by the INFN on the treatment of personal data;
- Are responsible for software packages that are installed on computers by those whom they allow access: originating with a detailed preliminary evaluation of software to be installed that does not have a regular license;
- Are bound to protect from unauthorised access the data used and/or stored in the computer and in the system to which they have access;
- Are bound to follow the instructions provided by the local INFN Computing and Network Service for regularly backing up their data;
- Are bound to protect their own account by choosing a sufficiently complex password and changing it periodically;
- Must not use the same password on different systems, nor communicate it or pass it on, nor give others the use of their account;
- Are bound to immediately inform the local INFN Computing and Network Service of any incident, suspected abuse or violation of security;
- Are bound, for the operating systems which they foresee using, to use updated antivirus programs, taking care to scan files that have been exchanged on the network and any removable storing media;
- Must not maintain unused remote connections nor leave the work station with unprotected open connections.

Violation of the rules

Any conduct contrary to legal norms or in violation of the rules set out in this document will result in the suspension of access to IT resources, following the communication of the the Director of the INFN center, and may have civil and penal consequences.