# RULES GOVERNING THE USE OF ICTP'S COMPUTING AND NETWORK FACILITIES

## I. INTRODUCTION:

1. This document defines the rules for the use of ICTP Computing and Network Facilities.
2. For the purpose of this document the term of ICTP Computing and Network Facilities includes:
   a) All personal computers, work stations, servers and peripheral systems such as printers, on the Campus site and directly or indirectly connected to the ICTP network, including the ICTP telecommunications network; with the exception of what provided in point IV.2 hereunder.
   b) All support services, program libraries, applications and any other software, document or service running on or related to any of the computers and above mentioned network, and all electronic mail and Internet services supported by ICTP computing facilities.
3. For the purpose of this document, the term "user" means any person making use of ICTP computing facilities.
4. For the purpose of this document the term "ICTP Computer Security Officer" (CSO) indicates a staff member explicitly appointed by the Director of ICTP to take care of the security of the ICTP computing and network facilities. The CSO may however delegate specific tasks to members of personnel of ICTS.
5. Infringement of the provisions of this document, and in particular any improper or malicious use of ICTP computing and network facilities, may cause material and/or moral damage to the Organization and serious problems for users of these facilities and may jeopardize computer security at the Centre.

## II. GENERAL POLICY

1. Authorization to use ICTP computing and networking facilities is at the discretion of the Director of the Centre.
2. The ICTP has computing facilities on its campus which are at the disposal of staff members and Consultants, for carrying out their official duties, as well as of Associates and all other categories of scientific visitors for carrying out their research tasks as well as for performing their scientific and administrative work. The personal use of the facilities, for all categories of users, is contemplated in the Annex.
3. The use of ICTP computing and networking facilities must cause no material or moral damage to the Organization, nor disrupt their operation.
4. ICTP computing and networking facilities must be used in conformity with:
   a) The collection of all Provisions, Guidelines and Rules of Use which is kept constantly updated by care of ICTS. The full package may be found in http://portal.ictp.it/icts/ictpguide/usage_policy/ or may be requested to ICTS.
   b) Any special instruction which ICTS may issue on specific matters.
5. Although the Centre endeavors to maintain and protect its computing facilities in the best possible way, it cannot guarantee their proper functioning or the confidentiality of information stored by them. The ICTP therefore accepts no liability for any loss of information or any breach of confidentiality.

## III. ACCESS AND USE OF COMPUTING FACILITIES

1. In order to have access to the computing facilities users must register themselves in accordance with the procedure in force. The mere fact, however, of using an ICTP account and/or of connecting to the ICTP network implies a tacit acceptance of these rules.
2. Accounts may only be used for the purpose for which they have been allocated to the user and for his own exclusive use.
3. All accounts must have appropriate access protection. The adoption of account codes or passwords, such as to ensure the single use of each account and the identification of each account with a single responsible user, is therefore compulsory.
4. The user shall take the necessary precautions to protect his personal computer or work station against unauthorized access. The user shall also protect details of his personal account, particularly by avoiding obvious passwords and shall not divulge his passwords to any third party, unless expressly authorized by his supervisor. Upon request from the responsible of ICTS the user shall select a new password.
5. If the user has been given an account with privileged access in connection with specific professional duties, he must advise the service manager concerned as soon as those duties no longer require privileged access.

6. The user must keep confidential all information obtained from access to ICTP computing facilities that the user may reasonably be expected to understand is confidential or sensitive in nature.
7. The user shall not seek unauthorized access to accounts which have access protection and shall not, except provided otherwise in point IV.1 hereunder, look for, disclose or exploit any security weakness in ICTP computing facilities or use these facilities to do so with respect to any other computing facilities external to ICTP.
8. The user must report any unauthorized use of his personal computer, work station or account to the ICTP Computer Security Officer (cso@ictp.trieste.it) or the Head of the Computer Section concerned.
9. Users shall respect the proprietary rights related to Software and Data available through the ICTP computing facilities, including licenses, copyrights and any other law or contractual agreement which restricts their use and distribution.

## IV. THIRD PARTY ACCESS TO USER'S ACCOUNT AND DATA

1. The ICTP Computer Security Officer shall have access to information contained in ICTP computing facilities. Such access is subject to the following conditions:
   a) The CSO shall not disclose this information unless this is expressly required for the execution of his/her duties.
   b) Access must always be consistent with the professional duties of the above-mentioned person and is only permitted for:
      (i) the resolution of problems affecting ICTP computing facilities, including upgrades or the installation of new facilities;
      (ii) the detection of computer security weakness or computer security violations;
      (iii) the monitoring of resources available to ensure the adequacy of ICTP computing facilities;
      (iv) the investigation of a suspected infringement of these rules by a user which, however, must be instructed by the Director. In case of emergency the same may be initiated by the CSO who, however, has to report to the Director as soon as possible;
      (v) the reallocation of access or deletion of accounts when a user's contract with ICTP is terminated or when his activities are no longer compatible with the aims of the Organization;
      (vi) the normal operations of the organic unit of the user where the absence of the user would seriously interfere with operations.
2. The ICTP Computer Security Officer, however, shall not have access to those data which are stored in privately owned computers temporarily connected to the ICTP network.
3. Some members of personnel of ICTS, delegated by the CSO, may also have partial access to information, but only in order to perform definite tasks specifically assigned to them by the CSO. On these occasions they are subject to all the limitations listed above for the CSO and,

in addition, they shall not exchange any information among themselves but they will uniquely refer to the CSO.

## V. LIABILITY AND SANCTIONS

1. The user concerned shall be liable for damage resulting from any infringements of the present document.
2. In any case of infringement of the present document, and as a general rule, the ICTP Computer Security Officer, the head of the Scientific Group concerned or the head of the service concerned shall inform the user responsible and explain the nature of the problem that has been detected or of the infringement that has been identified. If the incident occurs again, the user concerned shall be notified in writing by one of the above persons which of the provisions of this document have not been correctly applied. At any stage of this sequence the ICTP Computer Security Officer may, in the interest of the Organization and of the safety of the computer infrastructure, suspend the access of the concerned user to the ICTP computing facilities.
3. In the event of repeated infringement following the measures provided for under point V.2 above, or at any time in the presence of malicious intentions or when justified by the seriousness of the infringement, the Organization may withdraw access rights to ICTP computing facilities from the user concerned and/or initiate disciplinary and/or legal proceedings against him.

## VI. OFFICIAL DOCUMENTATION

This document is based on the UNESCO IT Security/Guidelines - AM9.3A, which covers other items not discussed. Please contact the ICTS helpdesk (*helpdesk@rt.ictp.it*) if additional information is required.