User Regulations of the Computing Infrastructure at the TIFR-CAM

Section 1: Scope

(1) These User Regulations shall apply to the use of the Computing infrastructure of the Tata Institute of Fundamental Research - Centre for Applicable Mathematics (hereinafter referred to as "TIFR-CAM"). The computing infrastructure shall above all include data processing equipment, communication systems and other facilities for computer-aided data processing, along with the attendant software.
(2) These User Regulations shall become binding on users who are not employees of the TIFR-CAM as well after having signed a pertinent commitment.
(3) TIFR-CAM employees can be required to comply with user obligations by way of general or individual office instructions. The binding nature of these User Regulations should also be ensured for employees through their signing of a pertinent commitment.

Section 2: Relationship to works agreements and the central works agreement

(1) To the extent that works agreements or the central works agreement lay down compulsory regulations governing protection rights or obligations for TIFR-CAM employees which diverge from these User Regulations, the provisions set out under works constitution law shall take precedence over these User Regulations.
(2) All users shall be obliged to comply with all rules applicable to use of computing infrastructure. This shall also apply in particular to users who are not TIFR-CAM employees, for example grant holders, visitors, fee recipients etc.

Section 3: Tasks of the Computer Centre (this refers to all computer equipment and the computer committee and employees and/or contractors engaged in all matters of maintaining and running the computer facilities in a smooth fashion)

(1) The computer centre of the TIFR-CAM shall perform the following main tasks:

1. Planing the TIFR-CAM's data processing facilities, implementation and operation of
2. Co-ordination of the procurement of data processing equipment
3. Acquisition, administration, documentation and care of standard software
4. User support

(2) The computer centre is moreover responsible for the planing, installation and operation of computer-aided information and communication networks, including the required networks, central servers as well as the data communication and telecommunication systems. In

this connection, the computer centre shall perform the following tasks:

1. Provision and upkeep of fault-free and, if possible, continuous operation of the communication network
2. Co-ordination of communication network extension and maintenance
3. Administration of address and name spaces
4. Provision of network services and central network servers (e.g. mail, WWW, news, fax and archive servers)
5. User support in the application of services
6. Implementation of security measures (e.g. protection against damaging software such as viruses; anti-relay and anti-SPAM measures for e-mails, firewall and the coding of sensitive data)

(3) The computer centre shall adopt the necessary technical and organizational measures to ensure that only persons with a valid user authorization will be able to use the computing infrastructure. If technically possible, the computer centre shall ensure that the use of the computing infrastructure will no longer be possible upon termination of a temporary user authorization.
The computer centre staff shall take care, within the scope of their tasks pursuant to paragraphs 1 and 2, that the pertinent rules of the applicable works agreements and the central works agreement are complied with.

Section 4: Rights and obligations of the computer centre

(1) The TIFR-CAM computer centre shall maintain a user file specifying user authorizations, including user and mail identification codes as well as the names and addresses of authorized users.
(2) The computer centre shall be authorized to deactivate and delete all of the user's data and programs upon termination of the user authorization. Deletion may only take place after having ascertained that the data will be of no further use to the institute.
(3) Following termination of the user authorization, incoming e-mails may be forwarded on request for the duration of six months to an e-mail address specified in writing by the user. If the user fails to specify any address, or upon termination of the three-month period, incoming e-mails will be rejected. If a further extension than six months for forwarding of e-mails is needed this request must be made in writing to the systems administrator
(4) If so required for fault elimination, system administration and extension, or for reasons of system security, as well as for the protection of user data, the computer centre may temporarily restrict the use of its resources or deactivate individual user IDs. If possible, the users concerned are to be notified in advance of any such actions.
(5) If there are concrete grounds to suppose that a user has acquired unlawful data access via the computing infrastructure, or that a user is storing unlawful contents on the computer centre's servers for his/her use, the centre may prevent any further use until implications have been sufficiently clarified. The same shall apply to any other contents that could lastingly harm the TIFR-CAM's reputation in public.
(6) The computer centre shall be authorized to adopt regular measures to review the security of system/user passwords and user data, and to carry out necessary protection measures (e.g. deactivate authorization in the case of easily decipherable passwords) in order to safeguard computing

resources and user data against unauthorized access by third parties. Should user-specific protection measures become necessary, the user is to be notified immediately.
(7) According to the following rules, the computer centre shall be authorized to document and evaluate the individual user's application of the computing systems - however, only insofar as this is necessary

1. to ensure orderly system operation or
2. to plan resources and administer the systems or
3. to protect the personal data of other users or
4. to account for expenses or
5. to detect and eliminate faults or
6. to clarify and prevent unlawful, in particular criminal, use.

(8)Subject to the conditions set out in paragraph 5, the computer centre shall also be authorized to inspect user files, with due regard to data secrecy, provided this is required to correct current faults, or to clarify and prevent any form of misuse. The inspection of message and e-mail mailboxes, however, is permissible only if this is imperative for current fault recovery in message services. In any case, such inspection must be documented and the user concerned must be notified immediately after the intended purpose has been achieved.
(9)Subject to the conditions set out in paragraph 5, the call and user data in connection with message circumstances of the telecommunication - but not the private contents thereof - may be recorded, processed and used. The call and user data in connection with online activities in the Internet and other teleservices which the computer centre provides to the user, or to which the computer centre provides user access, are to be deleted as soon as possible - at the latest, immediately after use, with the exception of account settlement data.
(10)According to the relevant statutory provisions, the computer centre is obliged to safeguard telecommunications and data secrecy.

Section 5: User authorization

(1) Users have the right to use the infrastructure within the scope of these User Regulations in accordance with the user authorization granted to them in writing (cf. paragraph 3 below).
(2) A claim to the use of the computing infrastructure does not exist, unless such claim was expressly granted by the TIFR-CAM under a separate contract.
(3) The user authorization for the computing infrastructure of the TIFR-CAM shall be granted by the computer centre only upon written application. The prescribed application form (Annex 1) shall be employed to this end. The application shall be accepted only if the form has been filled out correctly and the required user declarations have been given in writing.
(4) The user authorization may be granted for a limited period of time or restricted to a specific purpose. It may be fully or partially refused, or restricted, by the TIFR-CAM according to its reasonably exercised discretion. In particular, this applies if

1. a proper application has not been submitted or
2. the particulars provided in the application are incorrect (especially if incorrect specifications have deliberately been made) or
3. the user has violated his/her obligations under these User

Regulations in the past or there are sufficient grounds to suppose such a violation or
4. there are grounds to suppose that a user will not duly comply with his/her obligations under these User Regulations in the future.

Section 6: Withdrawal of the user authorization

(1) According to its reasonably exercised discretion, the TIFR-CAM may subsequently withdraw a user's authorization. Similarly it may subsequently restrict said authorization. Such withdrawal or restriction can be of a temporary, permanent or precautionary nature. The user application may be withdrawn or restricted above all if

1. users have violated these User Regulations, in particular the obligations set out under Section 7, or
2. users have abused the TIFR-CAM's computing resources to commit criminal offences or
3. users have through some other form of unlawful user conduct has been detrimental to the TIFR-CAM or
4. there are grounds to suppose that users will in future commit a violation within the meaning of items 1 to 3.

(2) The person concerned should be given the opportunity to state his/her own position prior to the withdrawal of the user authorization, provided the ultimate purpose is not jeopardized as a result. The person concerned may request the relevant committee to mediate. In any case, he/she should be given the opportunity to secure his/her data, provided their content is not of an unlawful or criminal nature.
(3) Temporary user restrictions may be repealed as soon as orderly use again appears guaranteed.
(4) A permanent user restriction or the complete debarment of a user from further use may be considered in the case of serious or repeated violations within the meaning of paragraph 1, especially if proper conduct is also not to be expected in the future.

Section 7: User obligations

(1) Users are required to refrain from any unlawful user conduct or conduct deemed inappropriate according to generally valid ethical standards. Over and above this, they are to refrain from any user conduct that could harm the TIFR-CAM's reputation in public.
(2) In particular, users are obliged to

1. observe the provisions of the User Regulations and to adhere to the restrictions specified in the user authorization;
2. to refrain from any action that is detrimental to the orderly operation of the TIFR-CAM's computer facilities;
3. to treat all data processing equipment, information and communication systems and other facilities of the computer centre with utmost care;
4. to work exclusively with the user ID codes permitted within the scope of the user's authorization;
5. to ensure that no other persons obtain knowledge of the user passwords and to take precautions to prevent unauthorized persons from accessing the DP resources of the computer centre, also including access protection via a secret and appropriate password,

i.e. which is difficult to decipher and is to be altered at regular intervals;

6. to refrain from ascertaining or using other persons' ID codes and passwords;
7. to refrain from the unauthorized accessing of other users' information and from passing on using or altering, without prior consent, any other users' information that may have become known;
8. to comply with the statutory regulations (in particular those governing protection by copyright) when using software, documentation and other data, this applying analogously to the contractual provisions (in particular licence conditions) under which software, documentation and data are provided by the computer centre;
9. to refrain from copying or passing on to third parties any software, documentation or data provided by the TIFR-CAM - unless this is expressly permitted by way of exception - or from using these for any purposes other than those allowed;
10. to refrain from any attempts on their own to rectify failures, damage or errors in conjunction with DP facilities and data media of the computer centre, but rather to report these without delay to the centre's staff;
11. to refrain, without the express consent of the computer centre, from interfering with the hardware installed by the computer centre and from changing the configuration of operating systems, system files, system-related user files and the network;
12. to refrain from installing any hardware or software without the computer centre's express consent;
13. to furnish, for controlling purposes, the heads of the computer centre with information on programs and employed methods and to allow them to inspect the programs, should they request this in well-founded exceptional cases - in particular on reasonable suspicion of abuse and for fault correction;
14. to co-ordinate any processing of personal data with the computer centre and – notwithstanding the user's own obligations under data prto take account of the data protection and data security precautions proposed by the otection law - computer centre.

(3) The following are condidered offences in particular:

1. Spying of data
2. Modification of data and computer sabotage
3. Computer fraud
4. Viewing/downloading/dissemination of pornographic depictions notably retrieval
   or possession of child pornography depictions
5. Viewing/downloading/dissemination of propaganda means employed by unconstitutional organizations
6. Defamatory offences such as slander or libel
7. Criminal infringements of copyright, e.g. as a result of the unlawful copying of software or publications
8. Frequent spamming of material not academic in nature

(4) The user shall be obliged to return to the TIFR-CAM, in an

appropriate form, all data, programs and documentation which the TIFR-CAM handed over to him/her or to which the TIFR-CAM has some other contractual or legal claim. Unless expressly agreed otherwise, the user shall not be permitted to retain copies of data, programs and documentation following termination of the user authorization.

Section 8: User liability

(1) The liability and indemnity obligations of users who are TIFR-CAM employees shall be subject to the liability provisions agreed by employment contract and to the general liability principles under labour law. The following paragraphs 2 and 3 shall apply to users who are not TIFR-CAM employees.

(2) The user shall be liable for all damages suffered by the TIFR-CAM owing to a culpable infringement of his/her obligations under these User Regulations.

(3) The user shall also be liable for damages resulting from third-party use of the access and user options granted to him/her, if he/she is accountable for such third-party use, especially in the case of disclosure of his/her user ID to third persons. In such case, the TIFR-CAM shall be able to demand a charge for third-party use from the user, with the assertion of any further indemnification claims not ruled out as a result.

(4) The user shall indemnify the TIFR-CAM from all claims asserted by third parties against the TIFR-CAM resulting from the user's culpable infringement of his/her obligations under these User Regulations.

User Application Form

The form should include the following particulars:

1. Name, address and signature of the applicant, as well as his/her status (e.g. employee, guest, grant holder, doctoral student etc.), along with details concerning any time limitations of the employment contract or other contractual relationship.
2. Description of the intended use or the planned project.
3. If applicable, particulars regarding the time limitation or other restrictions of user authorization; as a rule, it should be noted here that user authorization ends automatically with the termination of the employment contract or other contractual relationship.
4. Computer resources requested.
5. Declaration: the user recognizes the binding nature of the User Regulations (precise designation)
6. Declaration: the user undertakes to refrain from any inadmissible processing of personal data.
7. Reference: the user is to be made aware of the possibilities of documenting his/her user conduct and of inspecting his/her user files in accordance with the User Regulations.

The following declaration of agreement is to be emphasized explicitly in the application's form

8. Declaration: the user agrees to the processing of his/her personal data within the scope of the use of the computing infrastructure placed at his/her disposal (e.g. entry of his/her data in directories, telephone directory on WWW servers)