STANDARDS FOR COMPUTER LAB USE

Title IV. Security measures for the users of technological resources at UAB

Chapter I. General provisions

Article 40. Right to use the computer systems of the UAB

The computing resources of the Universitat Autònoma de Barcelona, both central facilities as well as the rest of the distributed facilities, including central/distributed systems, workstations, personal computers, internal and external networks, software, multi-user systems, etc., are for the exclusive use of the tasks of the University by members of their community or authorized people.

Article 41. Scope

1. Since most of the computer systems of the university are directly or indirectly connected with the overall network of the university, and that the misuse or lack of appropriate security systems in one of these systems may compromise the safety of other university systems or institutions to which the general network of the University is on, the content of this title applies to anyone who makes use of the university computer systems or systems available or directly connected networks or indirectly to the grid.

2. Persons applying or having access to the computer system or a connection from its system or network to the grid of the university shall know the security measures of computer resources, which will be available through the portal of the UAB.

3. The University reserves the right to take appropriate legal action when their rights are violated as a result of inappropriate use of the computer resources and make available to the competent authorities all the information available in case of complaints of misuse and violation of third party rights.

Chapter II. Computer systems

Article 42. Resource allocation of computer systems

For the allocation of the computer systems resources (institutional, departmental or central), and for the connection of systems and network to the grid, a responsible of computing resources and two categories of users are recognized: administrator of computing resources and end user.

Article 43. Head of computer resources

1. The person in charge of computing resources is the person who has to ensure the smooth operation of computer resources allocated under him always with the support of central and distributed services.

Article 45. End user

1. The end user is the person using a computer resource (private, donated by the UAB or propriety of the UAB) that is connected directly or indirectly to the overall network of the university.

2. The end user commits to follow the recommendations on the use of computing resources provided by the UAB, and the people in charge and managers of computer resources

especially in technical, data protection personal, material copyrighted and safety issues (primarily regarding the use of the network, updating the antivirus programs and policies on access and custody information).

3. The end user is bound to notify to the relevant responsible persons any change in the ownership of the computing resources assigned, and while this communication does not take place, remains solely responsible of all effects arising.

4 The person responsible for the computing resources, for reasons of breach of this policy, may refuse the use or access to a computer system, or the connection of a system or network to the overall network university. In case of network disconnection, previously will contact the person responsible to inform the appropriate action and solve problems.

Chapter III. Responsibilities of users

Article 46. Privacy, passwords and resource use

1. The users must take utmost care in the handling and use of computer equipment, and any additional infrastructure. They shall avoid undertaking any action, which voluntarily or involuntarily, may adversely affect the physical integrity of the machinery or plant (destruction, theft, unauthorized transfer, etc.) or the logical integrity of the software or data.

2. The users will access computer resources according to the specific regulations of each center, and will access to computer systems as recommended particular computer services and people resources managers have stipulated.

3. University computing resources are a public good and its purpose is to store, treat and use information related to the activities of the university. For security reasons, the administrator of the computer resources is able to inspect, ordinarily, the information contained in the computer systems. If, for safety reasons, need to make a more specific inspection, the administrator of the computer resources will have to justify it to the person in charge of computing resources.

4. User accounts on the computer systems of the university are personal and not transferable.

5. It is the user's responsibility to take utmost care of its password, for which, above all, will keep secret. The user will use passwords that are not trivial, and will change it periodically whenever he or she suspect or believe that their confidentiality can be raped.

6. All changes of passwords of the computer systems will be carried out making use of the mechanisms and protocols defined at the time by the people responsible for the systems.

7. The user agree not to use public resources (computers, network, connection points, etc.) for activities that are not strictly related to academic or research activities and will be his responsibility all the stored or downloaded copyrighted materials and without a license. In addition, the user is committed to respect the terms stated in the Ley orgánica 15/1999, of December 13th, of the protection of personal data and the UAB may take appropriate decisions on actions arising from these facts.

Article 47. Non-observance of community legislation

1. Is considered breach of the terms of use of computer resources the following cases:

a) The lawful use by third parties of user accounts on the computer systems (knowingly or not), both who conducts such as improper access as for the person responsible for the account.
b) Deprotection of the information of the users so as to facilitate a partial or general access.

c) Misuse of network services and electronic media to communicate with other users of computer systems, from the university network or networks to which the University is connected, as cause of discomfort (annoying messages or offensive, electronic harassment, impersonation of network addresses, etc.) or not the content of this title or regulations of the institutions and networks which is respected and through which to communicate. Also it will be considered a breach packet access communication to find out information which you do not own.

d) Searching for passwords of other people using any attempt to find and exploit security holes in computer systems from the university or outside, or using those systems to attack any computer system.

e) The creation, use or storage of programs or information that can be used to attack computer systems or outside the university.

f) The destruction, removal or transfer is not duly authorized to other units, any physical element of the computer installation or additional infrastructure.

g) Alteration of the integrity of the data.

h) Any other action that violates regulations or affecs the terms of use of computing resources.

Article 48. Applicable measures

1. The failure of the content of this title at any level will result in the suspension of access to computer systems, and or disconnection of the system or network to the grid of the University.

2. In cases of non-compliance, the people responsible for computing resources, after hearing the interested person, may apply preventively the measure provided in this article, although this measure must be confirmed by the Informatics Disciplinary Committee. In view of the facts and the circumstances, the committee will establish the duration and, if necessary, the frequency needed to confirm the action.

3. Against the decisions of this organ, interested persons may file an ordinary appeal to the rector or the person in which delegated.

4. The person in charge of computing resources may refer to the Informatics Disciplinary Committee cases which, although not explicitly referred to in this title, be considered punishable.

5. The measures referred to in this article shall apply without prejudice to disciplinary, civil or criminal actions that need to be applied to those suspected of involvement, as well as the repair of the damage.

OWN RULE OF OPERATION OF THE SID (Distributed Computing Service) FROM THE SCIENCE AND BIOSCIENCES FACULTIES

9. The use of computers from the computer labs is primarily aimed at teaching field. The use of applications outside this area is not allowed nor, in general, all that software which has not been installed by the SID technical staff. All special cases that make other necessary settings must be communicated to the SID responsible and duly authorized.

10. Any specific resource that is required must be applied only to the SID technical staff. It is not allowed to bringing out from the SID physical spaces any resource, hardware or software, or change its settings without express authorization. Also, both IP spoofing and unauthorized extraction of information from the network are forbidden. Neither can modify nor delete the system partition which is set to PCs.

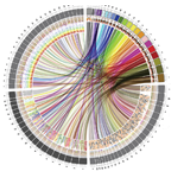
11. It is expressly forbidden, eating or drinking in the computer lab, as well as performing a playful use of computers. Keep areas clean and please take care of resources and respect the work of others.

12. SID users may send complaints or suggestions deemed appropriate by an email from the website of the SID itself or from an applet installed on each computer of the computerized classrooms.

Universitat Autònoma de Barcelona

UAB CEI CAMPUS D'EXCEL·LÈNCIA INTERNACIONAL

MSc in Bioinformatics



I, ...
have **read** and **accept** the terms and conditions of the **Standards for computer lab use** and the **Own rule of operation of the SID (Distributed Computing Service) from the science and biosciences faculties.**

In witness whereof, I sign this paper ..... day of ..... 20...