DECLARATION OF USE OF COMPUTER RESOURCES

Lecturer/Administrative or Support Staff/Student/Research fellow's Name:

_____

ID number: _____

University account: _____

***RedUGR* node (Ethernet address):** _____

I DECLARE THAT:

1. I am a user of the University of Granada's Computer Resources.

2. I agree to use these resources for University work only, according to the principles that inspire the Articles of Associations of the University of Granada.

3. I am familiar with the safety regulations for the users of Computer Resources of the University and I agree to comply with all the terms of the regulations.

4. I agree to always comply with the instructions and rules announced by the relevant University bodies and the current legislation.

5. I authorize the Computer Resources Manager to carry out the necessary technical operations on the Computer Resources used by the undersigned in order to ensure the safety and good performance of the Services provided to the University.

Date: _____

Signature: _____

UNIVERSITY OF GRANADA COMPUTER USAGE AND COMMUNICATION RESOURES REGULATIONS

(APPROVED BY THE GOVERNING COUNCIL ON JULY 7, 2003)

1. Scope of the Regulations

The Computer and Communication Resources (hereafter CR) Regulations aim to ensure that the resources are used for the purposes of Research, Teaching and Administration of the University of Granada. The Regulations also aim to:

1. Preserve the prestige and good name of the University of Granada as well as the prestige and good name of its Centres, Departments, Services, and Institutes.

2. Ensure the safety, performance and privacy of the systems and machinery of the University and its users.

3. Prevent situations that may result in any civil, administrative or criminal liability for the University of Granada.

4. Protect the work done by the RC technical staff from certain undesirable acts.

The University RC either dependent on the Centro de Servicios de Informática y Redes de Comunicaciones (centre for computer services and communication networks) – hereafter CSIRC – or on any other department, central systems, workstations, personal computers, internal and external networks, multi-user systems, communications services and etcetera are only for the performance of University tasks by the University members or authorized people.

Most of the University computer systems are connected to the general University network. Therefore, the misuse or the lack of proper safety systems may jeopardize the security of the other systems of the University or institutions to which the University network is connected.

As a result, these regulations apply to everyone using the Computer Systems, the Services they provide, or the Systems or Networks connected to the University network RedUGR. A copy of these regulations shall always be available for users and published on the University website.

Ignorance of these regulations is no excuse. The University reserves the right to bring legal actions in cases not covered explicitly by these regulations when they are provided in the Spanish Criminal Code or any other Spanish regulation. In this respect, the following regulations must be considered:

- Spanish Criminal Code: sections 263 to 267.a on hardware and software damage and sections 270 et seq. on intellectual property.
- *Ley orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal* (Spanish Organic Law 15/1999 of 13 December on the Protection of Personal Data): sections 43 to 49 on the confidentiality of information.
- *Ley 34/2002, de 11 de Julio de Servicios de la Sociedad de la Información* (Spanish Law 34/2002 of July 11 governing information society).

2. Assignment of computer system resources

There shall be a head for every Central or Department Computer System and two user categories: Computer Resources Manager and End-user.

2.1. Head of Computer Resources.

The Head of CR is the person in charge of the correct use of the resources under their protection:

- The CSIRC is responsible for the global management of the University Communications Network as well as all the Computer Resources and Services devoted to Centralized Administration, Research and Teaching. At the same time, they are responsible for the management, coordination and administration of the radio spectrum on the University premises.

- Deans and Heads of Centres are responsible for the general use resources devoted to Teaching in their centre.

- Heads of Departments, University Institutes and Research Groups are responsible for the CR of the members of such Departments, Institutes or Groups devoted to teaching or research.

- The Head of Computer Resources may delegate duties to control the use of CR.

2.2. Computer Resources Manager

The Computer Resources Manager is the person in charge of managing one or more CR (multi-user systems, workstations, personal computers, internal networks, databases, etc.) connected to the University network RedUGR. The CSIRC will be in charge of appointing the managers of all CR under their responsibility as well as the managers of teaching servers. The Heads of Computer Resources will appoint the managers of the resources described in point 2.1.

The CR Manager functionally depends on the Head of CR, to whom he will inform of every incident detected that may affect the good performance of the resources.

The CR Manager is obliged to accept these regulations applying to all the resources under his management. He must announce the regulations and impose them on every user depending on him. He will also impose the other specific regulations that may exist in this respect.

All CR Managers agree to follow the recommendations by the CSIRC regarding safety and to collaborate actively in the detection, monitoring and identification of potential violations of these regulations.

2.3. End-user

The end-user is the person who has any link with the University of Granada and uses the University Computer Resources or Services.

The end-user is obliged to accept these regulations since they began to use the University Computer Resources or Services. The end-user also agrees to follow

the recommendations by the CSIRC regarding safety and correct use of the resources. Any notification shall be forwarded to the user's e-mail address.

The end-user is obliged to inform the competent head of any change of title of the assigned resource. He will be the only person responsible to all intents and purposes until the notification is issued.

In cases of noncompliance with the regulations, the CR Manager reserves the right to provisionally refuse the application of a user to be part of the multi-user system or the connection of a system or network to the University general network.

3. User responsibilities

3.1. Data protection, passwords and use of resources

· Users must be careful when manipulating computer systems and additional infrastructure. They shall avoid voluntary or involuntary actions that may damage the installation (destruction, theft, unauthorized transfers, etc.).

· Users shall request access to CR following the specific regulations and they shall access computer systems following the recommendations by the CSIRC and the heads of resources.

· The University CR are public and aim to keep and manipulate academic, teaching, research or administrative information in line with the proper legal framework. For reasons of safety or computer services operational capacity, the CR Manager may usually monitor user accounts and resources of the University network RedUGR. The CR Manager must justify before the head of CR any extraordinary monitoring carried out for reasons of safety or computer services operational capacity.

· University users' computer accounts are personal and non-transferable and shall only be used for University teaching, research or administration.

· Users are responsible for their secret passwords and shall not use trivial or simple words. Passwords shall be changed periodically and any time users think their confidentiality may be breached.

· Any mandatory changes shall be made personally after the CR technical manager identifies the user.

3.2. Noncompliance with the Regulations

Noncompliance with the conditions of use includes the following:

3.2.1. Third parties accessing user accounts (user/password) in the computer systems (with or without the official user knowing) and the person responsible for that account, as well as the noncompliance with the University generic software licence.

3.2.2. The search of other users' passwords or any attempt to find and exploit safety breaches in the computer systems of the University or others, or using those systems to attack any computer system.

3.2.3. The creation, use or storage of software or information that may be used to attack the computer systems of the University or others, except by appropriate personnel to ensure the safety and operational capacity of the University network services.

3.2.4. The transmission of computer viruses, Trojan horses, worms, time bombs, or any other kind of malware.

3.2.5. The destruction, theft or unauthorized transfer to other premises of physical content of the computer installation or additional infrastructure.

3.2.6. The change, improper use or manipulation of data.

3.2.7. The misuse of the University network services (email, terminal emulation, interactive messaging, web, etc.) to communicate with other users of the University network or the networks connected to it when it results in:

· Illicit or illegal activities of any kind, especially spreading content considered to be racist, xenophobic, pornographic or sexist or to justify terrorism or attack human rights, and acting against the rights to privacy, to honour or to personal portrayal, or against human dignity.

· Spreading content against the principles of the Articles of Association of the University.

· Website spoofing.

· Compilation of others' information, including their e-mail address, without their consent.

· Phishing.

· Using the resources for propaganda and commercial purposes without express consent.

· Spreading false, incorrect or inaccurate statements or references about the University website and services, excluding any personal opinion on the institution.

3.2.8. Noncompliance with the CR security measures.

4. Measures to be implemented

Any noncompliance with these regulations implies preventive service suspension and/or temporary lockout of the RedUGR systems, accounts or networks in order to ensure the good performance of the University network.

The Governing Council will define the actions to be taken in case of noncompliance with any of the points in 3.2, without prejudice to the disciplinary, administrative, civil, or criminal actions that may apply.

5. The Computer Resources Committee

The Computer Resources Committee shall have the following functions:

· Ensuring the good management and performance of CR in the University of Granada.

· Suggesting the measures to be taken in case of noncompliance with these regulations. The committee may hear the parties involved before making a decision, ratifying or modifying the measures implemented by the CSIRC.

· Informing the Governing Council of the behaviours that may be subject to academic sanctions and/or have legal implications according to the current legislation.

· Suggesting to the Governing Council the possible measures to be taken in the situations not covered by these regulations.

· Listening to any complaint or suggestion made by University members.

· Suggesting to the Governing Council the change and update of these regulations when necessary in order to adapt them to technological developments.

· Yearly informing the Governing Council of the incidents that have occurred and the measures that have been taken.

· Developing the mandatory technical guidelines to ensure the good performance of the network and its services.

· Suggesting and setting up the Governing Council as well as updating a computer security incident directory. The directory shall include the corrective measures taken to deal with such incidents.