Rules regarding logins

All members of the UAM-CSIC Excelence Campus (referred as "the Campus" onward) have the right to have a login at the CCC-UAM.

When it comes to requesting a login, this must be done through the CCC-UAM webpage.

Every user must have an institutional email address managed by the UAM or the different institutes at the Campus. If this was not the case, documentation on their relationship with the Campus needs to be provided.

At any time documentation regarding the professional or academic relationship with the Campus may be requested from the user.

The duration of the account will be conditioned by the relationship with the Campus.

Those in charge of interns or visiting professors will be compelled to communicate the end of their relationship with the Campus should this happen before due time.

Users must indicate any change in their personal data: affiliation, address, telephone number and e-mail address.

When a login is generated, the user must retrieve it from the facilities of the CCC-UAM upon showing a valid identification (ID, Passport, UAM or institute’s card). Under no circumstance a password will be handed to third parties nor will be sent via e-mail.

If the password is not collected within seven days of having been communicated the creation of the login to the user, it will be considered null, and the account will be eliminated.

Passwords must be changed by the user at least once every six months. The password must be changed for the first time within seven days of it being handed.

If the CCC-UAM had any solid suspicions that any login might have been compromised, it might request the user a change of password and/or block it preventively.

User accounts must be dedicated to the development of research projects. These accounts will not execute applications with aims other than those contemplated by the CCC-UAM.

All applications installed by the user must be legal, and possess the corresponding usage license.

The usage of a login is restricted to a single person, and using them by more than one physical person is explicitly forbidden. The CCC-UAM will create as many logins as necessary so as to maintain the operability without sharing the login.

The usage of the CCC-UAM will be through the established access servers, completely forbidding logging-in through any other CCC-UAM server.

Only connections coming from equipment with IPs assigned by the Universidad Autónoma de Madrid, that is, IPs whose first two fields are 150.244. Any other access will not be permitted. Were it necessary to access from a different IP, one can rely on the VPN service provided by Information Technologies. However, it is worth mentioning that this service is offered by IT and is completely external to the CCC-UAM.
Running jobs outside the queueing system is completely forbidden, except for those graphical jobs whose nature disables them to being sent to the aforementioned queueing system.

The usage of graphical programs will be limited by time and percentage of CPU usage.

The maximum time of an inactive connection is 24 hours. After this time the connection can be closed any time.

To eliminate a login, this can be requested by e-mail to the administration staff of the CCC-UAM. Data regarding said login will be handed in exclusively to the login user, unless said user authorizes third parties to access these data.

Accessing other user’s data is forbidden, unless explicitly authorized by them.

Any violation of these rules, or bad practice on behalf of the user will entail a temporal or permanent block of the login, and even notifying the corresponding authorities of any kind of criminal activities.