RSMAS Network Account Application

University of Miami
rcf-staff@rsmas.miami.edu
Miami, Florida
305-421-4028

Classification:

☐ Staff  ☐ Faculty  ☐ Research  ☐ Lecturer
☐ Undergraduate  ☐ MPS  ☐ Graduate  ☐ Other: ______

Name:

CaneID:

Departmental or Group Affiliation:

Office/Building:

Phone Number:

Adviser or Supervisor:

I have read the Use of Accounts document provided with this application (over) and the policy document at http://www.miami.edu/index.php/a046_use_of_university_computing_facilities/
I understand and accept the guidelines there.

Signature:___________________________________________________    Date: _______________

Return completed form to the RSMAS Computing Facility, MSC 227. You will need to know your CNumber (UM ID number C########). Don't put it on this form.
Use of Accounts

The computing facilities of the Rosenstiel School of Marine and Atmospheric Science (RSMAS) are provided for the use of RSMAS students, faculty, and staff in support of the programs of the School. This account provides access to the RSMAS networked services. All students, faculty, and staff are responsible for seeing that these computing facilities are used in an effective, efficient, ethical, and lawful manner. These general policies serve as guidelines for their use.

1. Computer facilities and accounts are owned by the School and are to be used for school related activities only. Computer accounts are to be used only for the purpose for which they are assigned and are not to be used for commercial purposes or non-school related activities.

2. Accounts are for individual use only; they are not to be shared. The individual is responsible for proper use of the account, including proper password protection.

3. Programs and files are confidential unless they have explicitly been made available to other users. RSMAS Computer Facility (RCF) personnel may access others’ files when necessary for the maintenance of the computing systems. When performing maintenance, every effort is made to ensure the privacy of a user’s files.

4. Electronic communications facilities (such as MAIL and Web) are considered a privilege. Fraudulent, harassing or unlawful messages and/or materials are not to be sent or stored or copied.

5. No one should deliberately attempt to degrade the performance of a computer system or to deprive authorized users of resources or access to any of the computer systems.

6. Loopholes in computer security systems or knowledge of a password must not be used to damage computer systems, obtain extra resources, take resources from another user, obtain access to or change another user’s files, gain access to systems or use systems for which proper authorization has not been given. Users are prohibited from making any attempt to intercept or decode passwords or other access control information, or from making such information available to anyone.

7. Computer software and other material protected by copyright is not to be copied using School facilities or used, except as permitted by law or by contract with the owner of the copyright. Software subject to licensing must be properly licensed and all license provisions (downloading, installation, use, copying, number of simultaneous users, etc.) must be strictly followed.

8. When a process is consuming excessive system resources and objectionably degrading system response its resources may be altered without notice.