

HPC@UNM Account Usage Policy

11 April 2003
Version 1.1

James Prewett

Table of Contents

1 Preamble

This policy is a supplement to the University of New Mexico University Business Policies and Procedures Manual Section 2500. HPC@UNM does not provide general-purpose computing *per se*. It is a unique Center dedicated to leading edge computation and science. Accounts at HPC@UNM are provided to support your activities within the Center.

HPC@UNM maintains two sets of resources — HPC@UNM local resources and National Computational Science Alliance (Alliance) resources. The two are independent. Access to either of them must be obtained separately.

Aside from gaining account access, all HPC@UNM resources, including the local Alliance resources, are treated uniformly by this policy.

1. Where this local policy is more restrictive than UNM or Alliance policies, this local policy takes precedence.
2. Where the Alliance resources are being used and Alliance policies are more restrictive than either UNM or this local policy, the Alliance policies take precedence.
3. Where the UNM resources are being used and UNM policies are more restrictive than this local policy, the UNM policies take precedence.

2 Network Security Officer

To assist in enforcing this policy, HPC@UNM has designated a *Network Security Officer*. This person is a full-time system staff member whose duties include overseeing network and system security.

The name of HPC@UNM's security officer is posted on the bulletin board at the front desk of HPC@UNM. This person can be contacted [via email](#) or [via the web](#).

3 Obtaining an Account

HPC@UNM provides two kinds of accounts — HPC@UNM local accounts and National Computational Science Alliance (Alliance) accounts. The two are independent. Access to either of them must be obtained separately.

3.1 HPC@UNM Local Accounts

Instructions for requesting HPC@UNM local accounts can be found on our [primary website](#).

In order to receive an account, you must have a designated sponsor. Sponsors are drawn from the HPC@UNM staff and associated faculty. Your sponsor must approve your request. The systems staff must also approve your request. Your account can be restricted or closed at the request of your sponsor.

3.2 NCSA Alliance Accounts

Instructions for requesting Alliance accounts can be found on our [primary website](#).

To obtain an Alliance account, you must either be joining an existing Alliance project, or you are proposing a new project. The web-based form allows either option.

If you are joining a new project, your request must be approved by the Principal Investigator (PI) of the project (or her delegate) as well as by the systems staff.

If you are proposing a new project with yourself as PI, your project must be approved by a local allocation board as well as by the systems staff. This board will work with you to define your project and to establish your project as an Alliance project. Local Alliance projects are currently limited to 10,000 service units of time on the Alliance clusters. As your use approaches that limit, you will be encouraged to apply for a larger Alliance allocation.

3.3 Closing an account

If your project completes, or if your participation in an Alliance or HPC@UNM project ends, you are responsible for closing your accounts at HPC@UNM. Closure of accounts is part of the normal exit process if you are ending your employment by HPC@UNM.

Accounts that are not used for 3 months may be “frozen” — their passwords locked and access denied. Before an account is frozen, you will receive notice via your normal email address. Notice will be sent at least 48 hours before the account is locked. If your account is frozen, your PI or sponsor will also be notified by electronic mail.

Frozen accounts can be restored by contacting the HPC@UNM help desk via [the web](#). When the account is unfrozen, the account password will be restored to your default password, and the account owner will be notified by electronic mail.

4 Acceptable Use of Your HPC@UNM User Account

The use of HPC@UNM computing services is a privilege. Users who have been granted this privilege must use the services appropriately, ethically, and lawfully. Violations of UNM policies or HPC@UNM policies may result in your access to these services being terminated with or without notice.

4.1 Responsibilities

As a user of the HPC@UNM system, you are responsible for your account. This includes, but is not limited to, all usage of your account and all contents of your account. HPC@UNM will not be responsible for the usage of your account.

4.1.1 Contents

You are responsible for all contents of data stored under your account.

4.1.2 Sharing Accounts

User accounts may not be shared without prior permission from the administrative staff.

Most of the benefits of sharing an account can be obtained by sharing a common group, and/or using commonly available tools such as CVS to share files. Feel free to discuss alternative possibilities with the systems staff.

Passwords may not be shared with anyone. The only exception is when an account is being shared between multiple people with appropriate authorization.

If you feel you must share an account for some reason, you must obtain prior written authorization from HPC@UNM's designated network security officer See [\(undefined\) \[Network Security Officer\]](#), page [\(undefined\)](#).

Administrative accounts may be shared among HPC@UNM Systems staff and student employees. Access to administrative privileges, even among systems staff, is on a need-to-know basis.

4.1.3 Lost Passwords

Users are provided an initial default password in their new user packet. You should change your password the first time you login and periodically thereafter. If it is necessary for you to request a password change from us (for example, when you have forgotten your current password), your password will be set to this default. It is important that you keep this form in a secure place for your reference.

If you have lost your default password, you will be required to wait until a duplicate can be mailed to you via U.S. mail. HPC@UNM does not provide passwords by phone, fax, or electronic mail.

4.1.4 Password Requirements

Passwords must be at least 8 characters in length with no repeats. The user's name must not appear as any part of the password. The password must contain at least 1 character from each of the following sets:

Lowercase letters

‘a - z’

Uppercase letters

‘A - Z’

Digits ‘0 -- 9’

Special characters

any printable character not listed above except double quotes (‘‘’), single quotes (‘’), backtick (‘`’), and backslash.

Passwords should *not* be dictionary words, reverses of dictionary words, or be easily guessable.

Users should make it a practice to regularly change their passwords. No password should be used for more than 3 months. HPC@UNM reserves the right to enforce this policy by mandating password changes.

Adherence to this policy will be spot-checked with standard password-breaking security programs. If your password is vulnerable, you will be informed and requested to change it within 48 hours. HPC@UNM reserves the right to lock your account if the password is found vulnerable and you do not remedy the problem within the time limit specified.

4.1.5 Storing Passwords

Passwords (for any system, HPC@UNM or otherwise) should not be stored on any computer system on the HPC@UNM network without using strong encryption to protect them (e.g. Blowfish or PGP encryption). Strong encryption is considered to be any encryption algorithm that provides at least 128 bits of security.

If you *must* store a password in a file that is not encrypted, ensure that

1. The file is stored on a local (not shared) disk on your laptop or workstation.
2. The file is properly protected using user and group permissions.

HPC@UNM is currently supporting GNU Privacy Guard (GPG) on Unix/Linux workstations. You are encouraged to create a GPG key and share the public portion of the key with the Center via a key server. Instructions for creating and using your key, and for using the key server can be found on [the HPC@UNM security web page](#).

4.1.6 Compromised Password

If you suspect that your password has been compromised, for any reason whatsoever, change it immediately using a *secure* channel! Also, this incident should be reported via email to the Center's [network security officer](#).

4.1.7 Attempts to Gain Unauthorized Access to Accounts or Data

Any activities whose primary or incidental goals would result in gaining unauthorized access to accounts, personal data, or passwords are strictly prohibited unless authorized in writing by HPC@UNM's network security officer. Examples of such activities include running password cracking programs, network sniffers, trying to guess passwords, *etc.*

4.1.8 Attempts to Undermine Security

You may not download, install, or run software whose purpose, express or implied, is to reveal or enable security weaknesses without the written approval of HPC@UNM's security officer.

4.1.9 Commercial Use

The HPC@UNM network is for use in support of activities directly related to your position at HPC@UNM. You may not use this account for commercial purpose without written approval from the Director.

4.1.10 Copyright Infringement

You may not use your account for storing or distributing software or other copyrighted products without having a proper license to do so.

4.1.11 Proprietary software and data

You may not access, alter, copy, move or remove proprietary information, proprietary software or other proprietary files (including, but not limited to, programs, members of subroutine libraries, data, and electronic mail) other than your own without prior authorization from the appropriate system administrator, security officer, or other responsible party. You must not copy, distribute, display, or disclose third-party proprietary software without prior authorization from the licensor. Proprietary software must not be installed on systems not properly licensed for its use.

4.1.12 Disrupting Service

You may not intentionally disrupt service to any machine on the HPC@UNM network. You also may not use any machine at HPC@UNM to disrupt service to any other machine at any location. Repeated inadvertent disruption may also be grounds for action.

4.2 Email and Electronic Communications

Electronic communications include, but are not limited to e-mail, data, audio, video, and text that is conveyed or stored electronically. These communications may be a part of your function at HPC@UNM, or they may fall under See [\[Incidental Personal Use of Computing Services\]](#), page [\[undefined\]](#).

4.2.1 Restrictions on Electronic Communications

The following are examples of electronic communications that are discouraged:

- copyright law violation
- chain letters, pyramid schemes, and unauthorized mass mailings
- fraudulent, threatening, defamatory, harassing, or illegal materials
- non-work or non-class related information sent to an individual who has explicitly requested that the information not be sent
- commercial or personal advertisements, solicitations, or promotions

Please do not post or otherwise originate these items from your account.

4.2.2 Email Privacy

Because you are responsible for all contents of your account, the HPC@UNM systems staff will not view your email, or give others access to your email, except in extreme circumstances including a well-founded need to protect the integrity of the systems.

For personal email to be searched by UNM staff, a search warrant or written authorization by a president or vice-president of UNM must be obtained.

4.2.3 Abusive, threatening and harassing e-mail policy

Don't send it. Report it to the [security officer](#). Include a copy of the message with full and complete email headers. If you feel physically threatened you should also contact UNM Police at 505.277.7872.

4.2.4 Spam

Don't send it. Try not to read it.

HPC@UNM is committed to reducing the volume of spam by providing filtering at the point of arrival and by supporting user-specific filtering. See <http://www.hpc.unm.edu> for more information.

4.3 Incidental Personal Use of Computing Services

The HPC@UNM allows *de minimus* incidental personal use of computing services. Such use must not interfere with an employee fulfilling his or her job responsibilities, interfere with other users' access to resources, or be excessive or inappropriate as determined by management.

You may not use the computers for anything that may be found offensive or inappropriate to others in your office. See [UNM's Acceptable Computer Use Agreement](#) for further elaboration.

4.4 Privacy

All users shall respect the privacy of others. This includes all users, administrators, and management staff.

Privacy and monitoring policy at HPC@UNM are those specified in [UNM's Acceptable Computer Use Agreement](#) for further elaboration.

5 Security Incidents

To ensure network security, we need every user's help. If you suspect that a machine has been compromised, contact the network security officer. The name of HPC@UNM's security officer is posted on the bulletin board at the front desk of HPC@UNM. This person can also be contacted via **email** or by the World-Wide Web at <http://www.hpc.unm.edu/security/>

6 System Administration

6.1 Staff Administration

Most systems at HPC@UNM are administered by the HPC@UNM systems group. This allows us to keep control over various issues, including security and compatibility. Prior authorization must be obtained in writing from the HPC@UNM network security officer (See [\[Network Security Officer\]](#), page [\[undefined\]](#).) if a machine is not to be maintained by the systems group.

6.2 Self Administration

We recognize that under certain circumstances, it may be required that a machine not be administered by the HPC@UNM systems staff.

If you can justify having administrative access to one or more HPC@UNM resources, your request must be submitted in writing to HPC@UNM's network security officer (See [\[Network Security Officer\]](#), page [\[undefined\]](#).). To gain such access, your request must be approved by both the network security officer and the Associate Director in charge of systems.

6.2.1 Self Administration Authorization and Responsibility

Prior authorization must be obtained in writing from the HPC@UNM network security officer if a machine is not to be maintained by the systems group. The systems group is not responsible for any machine that they do not maintain, except to prevent problems with shared resources, such as the network.

If you take on administrative responsibilities for a machine or resource, you agree to be fully responsible for any issues or problems that occur on that machine or resource, or are engendered by your actions.

If you are granted the right to administer your own system, the systems group will be responsible for making a backup of the system, sufficient to restore the system to the point at which you are taking responsibility.

Subsequent backups of your system will have to be arranged with the systems group if you elect to have backups created.

6.2.2 Audit Policy

The systems group reserves the right to audit the machine at any time utilizing any reasonable method, including, but not limited to, security audits.

Specifically,

HPC@UNM reserves the right to check the permissions of files owned by users.

HPC@UNM reserves the right to check the contents of files owned by users that materially affect the security of HPC@UNM or other computing systems. Such files include, but are not limited to, `‘.netrc’`, `‘.rhosts’`, and `‘.shosts’`.

HPC@UNM reserves the right to scan machines on the network for possible security loopholes, weaknesses, or policy violations.

6.2.3 Administrator Access

The systems group must have administrator level access to all machines residing on the HPC@UNM network. This access will be used only in extreme circumstances, or with prior approval from the group administering the machine. However, administrative access must be provided to the HPC@UNM systems group at all times.

6.3 Removing Machines from the Network

Machines may be removed from the network without notice for reasons related to network security, or excessive consumption of HPC@UNM resources.

6.4 Personal Machines

Personal machines that are connected to the HPC@UNM network for less than 24 hours, or that reside in the building less than a week are subject to all policies regarding Self Administration except that their administrators need not obtain prior authorization to administer them, and their administrator passwords need not be given to the systems staff unless the systems staff requests this password. This time limit refers to the total accrued time that the machine is able to access network services or is present in the building. See [\[Self Administration\]](#), page [\[undefined\]](#).

Personal machines put on the HPC@UNM network for periods greater than or equal to 24 hours or which reside at the Center for a week or more must be authorized by the HPC@UNM network security officer See [\[Network Security Officer\]](#), page [\[undefined\]](#). The Administrator password must be given to the systems staff.

All personal machines are subject to audit by the systems staff.

Table of Contents

1	Preamble	1
2	Network Security Officer	2
3	Obtaining an Account	3
	3.1 HPC@UNM Local Accounts	3
	3.2 NCSA Alliance Accounts	3
	3.3 Closing an account	3
4	Acceptable Use of Your HPC@UNM User Account	4
	4.1 Responsibilities	4
	4.1.1 Contents	4
	4.1.2 Sharing Accounts	4
	4.1.3 Lost Passwords	4
	4.1.4 Password Requirements	4
	4.1.5 Storing Passwords	5
	4.1.6 Compromised Password	5
	4.1.7 Attempts to Gain Unauthorized Access to Accounts or Data	5
	4.1.8 Attempts to Undermine Security	6
	4.1.9 Commercial Use	6
	4.1.10 Copyright Infringement	6
	4.1.11 Proprietary software and data	6
	4.1.12 Disrupting Service	6
	4.2 Email and Electronic Communications	6
	4.2.1 Restrictions on Electronic Communications	6
	4.2.2 Email Privacy	7
	4.2.3 Abusive, threatening and harassing e-mail policy ..	7
	4.2.4 Spam	7
	4.3 Incidental Personal Use of Computing Services	7
	4.4 Privacy	7
5	Security Incidents	9

6	System Administration	10
6.1	Staff Administration	10
6.2	Self Administration	10
	6.2.1 Self Administration Authorization and Responsibility	
	10
	6.2.2 Audit Policy	10
	6.2.3 Administrator Access	11
6.3	Removing Machines from the Network	11
6.4	Personal Machines	11