GFDL Computer Use Policy

Introduction

The computing facilities at GFDL are provided in order to support the scientific mission of the laboratory. All use of the computing systems at GFDL should be in accord with this underlying purpose. It is in this light that this policy statement is presented.

This document defines the policies for users of GFDL's scientific computing network. GFDL's network consists of a supercomputer, workstation servers, desktop workstations, and network routers linked together by a local area network. The network does not include any of the standalone personal computers that are not connected to the network. Because of the nature of the tasks that administrative computers perform and the sensitive and confidential information they contain, policies for these systems are covered elsewhere and are beyond the scope of this document.

This document contains the following sections: authorized use of the system, system and data integrity, responsible use of the system, communications, remote access users responsibilities, and password policy.

Failure to abide by these policies may constitute grounds for termination of access privileges, administrative actions such as disciplinary actions, and/or criminal prosecution, if warranted.

Authorized Use

The GFDL scientific computing facility is provided to GFDL scientists and support staff and individually authorized outside research collaborators for the purpose of advancing the Laboratory's scientific research mission. The distribution of computing resources among scientific projects and support groups is subject to review and approval by the GFDL Director, based on the quality of the proposed scientific research and the likelihood that the activities will contribute to the Laboratory's mission objectives. Authorization for access and use of Laboratory computing facilities by anyone outside GFDL rests solely with GFDL Management.

Because of the above requirements, users of the GFDL scientific computing facility must observe the following policies:

Everyone who is authorized to use GFDL's computer facility will be assigned a unique account of his/her own. This account, and the associated password, is intended to be used by that person alone and may not be shared with any other person. There is no reason to give your password to another user or to use another person's password and account. There can be no exceptions.

The selection of a password should be taken seriously. Requirements for selecting a suitable password are provided in the Password Policy section. All users must change their password at least every 90 days. It is your responsibility to maintain the confidentiality of your password.

If you suspect that someone has discovered your password and is using it to access the system, you will be expected to take the following action:

1. Change your password immediately.

2. Notify someone in the systems group as soon as possible.

Liability

Users are responsible for reading and understanding the applicable NOAA/GFDL regulation(s) and will comply with the provisions contained therein. It is the user's responsibility to understand the security rules governing the use of system accounts. Users are liable for the loss of, or any damage to, the system, its hardware components, and software if said loss or damage should occur as a result of willful misconduct, negligence, or deliberate unauthorized use. Further, users are liable for any damage caused by, or resulting from, the use of their system account. Users are subject to legal action should it be determined that they are found responsible for damage to, or loss of, DOC assets through use of their system account.

System and Data Integrity

In order for a computer system to be considered a useful and productive tool, there must be certain assurances that the system will be reliable and available. There are several approaches that can be taken to assure system and data integrity. In a scientific research environment, you want to minimize the difficulty in sharing information while at the same time maximizing ease of use. Every operating system has some mechanism for providing system and data integrity. However, system and data integrity is largely accomplished through respecting other people's rights and privacy. The following are issues and policies that affect system and data integrity. This list is by no means exhaustive. Common sense and ethical judgment, in most cases, is all that is needed.

- System Modifications
  Only authorized personnel shall modify, install, or remove any hardware. Any and all hardware maintenance will only be performed by authorized maintenance personnel. Users should only reboot or reset computer related equipment and peripherals when specifically told to do so by someone in Operations or Systems.
- Inactive Workstations
  It is important that each office user should log out of his/her office workstation at the end of the day. This is important, not only for reasons of security but also to simplify recovery if the network should go down. Public users must obviously be sure to log out when they have finished their workstation session. For reasons of security, users must lock their workstation screen (using a lock-screen command) when leaving their workstation unattended for some period of time.
- Software
  All third-party software installed and used will be purchased and/or licensed. The only exceptions are software packages that have been placed in the public domain. All copyrights will be honored. For your own protection, never run a program given to you unless you know what it does and completely trust the source.
- Data and Files

While it has always been the case that access and read permissions are implicit on all files, it should be noted that arbitrarily reading another user's files may not necessarily be harmless and might well cause problems for the owner of the files. Users who wish not to have their files publicly accessible should change the permissions on their files to disallow general access. Everyone wanting to modify or delete files owned by another user must first get explicit permission from the owner of those files. Lack of file protection does not give anyone the right to modify or delete another's files.

- Administrative Privilege
  Administrative privileges (e.g. root or "superuser" access) are only given to authorized personnel. No one should attempt to gain administrative privileges for any reason. In general no user should attempt to gain additional privileges or access other accounts.
- System Problems
  Users should make every effort to report any new systems problems to someone in Operations or Systems. These problems can only be resolved if Systems/Operations are made aware of them. Likewise, computer facility personnel will make every effort to keep users informed of the status of the systems and any systems problems as they are identified.
- Sensitive & Confidential Information
  Since there is no provision for keeping sensitive and confidential information on GFDL's scientific network, all information kept on the network is considered neither sensitive nor confidential. If you choose to keep information on the network that in other contexts would be considered sensitive or confidential, please be aware that, by having this information on the network, you are, in effect, desensitizing the information.

Responsible Use

In order to maximize the utility and flexibility of the computing environment, it is desirable to minimize the number of rules placed on individual users. Such an environment requires, however, that all users be responsible in their use of the computing system. This sense of responsibility entails using appropriate computing resources both in an efficient manner and with regard to the computing welfare of the system and of other users. The term "responsible" is quite subjective in this context, and varies from situation to situation. It is the attitude that is more important than any set of rules. It implies, strongly, however, that all users bear a portion of the responsibility for the overall health of the computational environment.

Some examples of issues related to responsible use:

- Using the resources appropriate for the task. For example, it would be inappropriate to use a high-end public graphics workstation for word processing if other resources are available for word processing.
- If a task would place an extraordinary drain on system resources, effort should be given to create and implement a more efficient means of accomplishing the goal. For example, accessing large amounts of data in an inefficient manner can have a very serious negative impact on the entire computing system. It would be "responsible" to attempt to accomplish the underlying task in a more efficient manner. An alternative might be to schedule the task for execution at a time when the system is under minimal strain.
- No user should knowingly interfere with the use of the system by another user without express consent of that user. An example would be using the resources of someone else's

workstation without their permission. It should be emphasized that there are few "hard and fast" rules regarding responsible use of the computer system. Rather, what is important is awareness by all users that efficient and harmonious use of the system is in everyone's best interest.

Communications

Computer networking has revolutionized communications, both internal and external to the lab. The power and ease of electronic mail and data transfer have increased our scientific productivity. As with any revolution, there is potential for abuse. The following are a few policies whose aim is to curb any potential abuses (not to inhibit appropriate use).

- Computer assisted communication (for example, electronic mail) is a privilege and not a right. It is not to be used for messages that are political, ideological, or commercial in nature.
- Messages that are offensive, threatening, harassing, or obscene in any sense are not acceptable.

Password Policy

1. Passwords must be created consistent with the following criteria:
    - Passwords must have at least eight (8) non-blank characters; and
    - At least one of the characters must be from the alphabet (upper or lower case); and
    - At least one of the characters must be a number (0-9) or a special character (e.g., ~, !, $, %, ^, and *); and
    - Six of the characters may only occur once in the password (e.g., 'AAAAAAA1' is not acceptable, but 'A%rmp2g3' and 'A%ArmA2g3' are acceptable); and
    - Passwords must not include any of the following: vendor/manufacturer default passwords: names (e.g., system user names, family names), words found in dictionaries (i.e., words from any dictionary, spelled forward or backward), addresses or birthdays, or common character sequences (e.g., 3456, ghijk, 2468).
2. Passwords in readable form (e.g., written on paper) must be kept in a safe location and not stored in a location accessible to others. For example, safe locations include storage in a locked container accessible only by the user.
3. User applications must not be enabled to retain passwords for subsequent re-use, or be configured to bypass authentication mechanisms. For example, Internet browsers must not be enabled to save passwords for re-use.
4. Passwords must not be distributed through non-encrypted electronic mail, voice-mail, or left on answering machines.
5. Passwords must be changed as follows:
    - At least every 90 days,
    - Immediately if discovered to be compromised or one suspects a password has been compromised,
    - Immediately if discovered to be in non-compliance with this policy, and
    - On direction from management.
6. Do not reuse a password you have used any of the last 8 times you have changed your password, or more recently than 2 years from when you last used the password.
7. Users who do not change their password using yppasswd after the 90 days has expired will have their accounts suspended until they call operations (609-452-6560) or e-mail

oar.gfdl.help@noaa.gov requesting to have their account reactivated and must change their password during their first login session.

Remote Access Users Responsibilities

Because remote users are crucial to effective remote access security, all DOC federal employees and contractors must follow the mandatory minimum standards of this policy. Failure to comply with this policy may result in disciplinary action and/or revocation of remote access privileges as determined by their manager, supervisor, or COTR. Remote users must:

- Complete initial and refresher IT security awareness training as required by DOC IT security policy.
- Certify that he/she have read and understand their responsibilities under this policy prior to receiving remote access authorization and authentication credentials. Abide by the terms of signed "remote access user security agreement."
- In accordance with operating unit CIO's remote user assistance program, ensure the computer used for remote access is configured and maintained according to this policy and according to the method of remote access being used.
- Periodically check to determine that all applicable security patches available for the software used to process DOC information on personally-owned computers have been installed.
- Return DOC-owned computers used for remote access as directed by the responsible system owner, manager, supervisor, COTR, or ITSO so that the security configuration (e.g. patches) of the computer can be checked and enhanced.
- Exercise caution when accessing government information from a public area to prevent compromise of sensitive information.
- Report, within 24 hours of identification, all IT security incidents to their supervisor, to their COTR, to their ITSO, or to the responsible CIRT following DOC incident reporting procedures (http://www.osec.doc.gov/cio/oipr/ITSec/Incihand.htm).
- Users should protect remote access machines with password-protected screensavers, that auto start after a maximum of 15 minutes of idle.
- Users will not share their remote access account/token card.
- Without explicit permission, users will not bridge networks or provide gateway/proxy access into GFDL's network or servers.
- Use of public-access (e.g. cyber cafes) equipment is prohibited.
- Users who do not remotely access GFDL via their CRYPTOCard token card for 90 days may temporarily have their remote access account suspended until they call operations (609-452-6560) or e-mail oar.gfdl.help@noaa.gov requesting to have their account reactivated.

Web Page Policies

A comprehensive list of policies can be found at:
http://cobweb.gfdl.noaa.gov/policies