This document is one of a set that provides general information about CNS services and facilities. This document includes a CNS organizational overview, who to contact for help, CNS hardware and facilities, information about accounts, userids and passwords, accounting and charging information, and a brief summary of the CNS charging algorithm.

For information about available software, see the "General Information: CNS Software and Software References [http://docweb.cns.ufl.edu/docs/d0009/d0009.html]" document (D0009).

For information about newsletters, handouts, manuals, seminars and workshops, and other sources of information, see the "General Information: Sources of Information on Computing [http://docweb.cns.ufl.edu/docs/d0008/d0008.html]" document (D0008).
Table of Contents

Userids and Passwords ........................................................................................................3
Userids ....................................................................................................................................3
Your Password ......................................................................................................................3
System Access Limitations .....................................................................................................5
Misuse of Services ..................................................................................................................5
Userids and Passwords

This chapter describes userids and their password protection. For information on how to obtain a userid and password, refer to the chapter entitled "Obtaining CNS Userids [http://docweb.cns.ufl.edu/docs/d0007d/d0007d.html]."

Userids

To use most of NERDC's services (except for LUIS and DOCWEB), you must have a CNS computer userid. Your userid enables you to run batch jobs, sign on to and use interactive systems, store data in the computer system, use the CNS Dial-Up Server, purchase computing services and supplies, print output on special types of paper, and use electronic mail on BITNET or the Internet. Other services (such as consulting and programming) also require a valid userid to which these services can be charged.

Note

Users considering using the UF/CNS dial-up service should be aware that this service is under review, and may possibly be discontinued at or shortly after the end of calendar year 2006. For more information, please see Dr. Hoit's memo to Deans, Directors and Department Heads of 05/02/2006, titled Charging for UF Dialup Services [http://www.admin.ufl.edu/ddd/default.asp?doc=11.11.1920.1].

When you open an account with NERDC, you are assigned an initial userid. Userids may be from one to seven alphanumeric characters, and no two userids may be identical. The userid will be the same for all CNS systems (except possibly AIX).

Your Password

When you access most of NERDC’s systems, you are required to supply a password with your userid. A password is required for your protection. When you sign on to an interactive system (such as TSO), it will prompt you for your password. The format of the password and the entry method depend upon the service that you are trying to access.

CNS system passwords must contain five to eight characters and must begin with a letter. Certain obvious passwords, such as "secret" and "password," will be rejected by the system. Passwords that match the userid will also be rejected.

Two concerns are involved in regulating access to system resources and capabilities.

- The first concern is protecting you and your funds. If you give the system an incorrect password, access will be denied.
- The second concern is limiting you to a specific amount of processing. System access limitations are described in the "Obtaining CNS Userids [http://docweb.cns.ufl.edu/docs/d0007d/d0007d.html]" chapter in this manual.
Changing Your Password

You are required to change your password at least every six months. However, we strongly encourage you to change it frequently (every several weeks).

The intent behind requiring you to change your password is to reduce the risk of passwords to accounts falling into the wrong hands and to encourage you to protect your account against unauthorized use through frequent password changes.

A password is valid for only six months (or some other department-selected interval not to exceed six months). During the days before your password is due to expire, you will receive warning messages when you sign on or in your batch job log. If you allow your password to expire without changing it, you will not be permitted to sign on. To have your expired password reset, first contact your departmental computing coordinator or university computing support organization. If you do not have a departmental computing coordinator, contact CNS Accounting Services (109 SSRB, (352) 392-2061). We strongly recommend that you change your password more often than this.

In the following cases, you must have CNS Accounting Services reset your password:

- If you cannot remember your password
- If you receive an "ACCESS DENIED" message after your password has expired when you attempt to sign on or submit a batch job
- If you have exceeded the daily password violation count (the system limits the number of unsuccessful sign-on attempts)

To access interactive services, you must enter your password in response to a prompt. On full-screen workstations and through protocol converters, the system will prompt for password entry in a field that will not be displayed. This lessens the possibility that another person might observe the entry of your password.

When you sign on to any interactive service and change your password, at that time you will be required to enter the new password a second time to verify that it is to be changed and was typed correctly. This requirement minimizes the possibility of inadvertently changing a password to an unknown value.

In addition, whenever a password is set by anyone other than the person to whom the account has been assigned, either by request or when the account is created, the password must be changed at the next interactive or batch access.

See How to Change Your CNS Password (D0005) [http://docweb.cns.ufl.edu/docs/d0005/d0005.html] for information on changing passwords through different systems.

Responsibility for Your Password

The password associated with your userid is your only protection against unauthorized use of your userid. You are responsible for changing your password frequently. You are also
responsible for ensuring that a password is never stored in any file or data set.

CNS is not responsible for unauthorized access caused by your negligence. CNS will actively cooperate with you, however, to determine the source of continuing unauthorized access.

Anyone who suspects unauthorized use of a userid should first run a CHRGLIST job to investigate questionable charges. To use CHRGLIST see the online interactive CHRGLIST utility at http://www.cns.ufl.edu/utils/. You can also refer to NERDC's Utilities: How to Use the CHRGLIST Utility document (D0083) [http://docweb.cns.ufl.edu/docs/d0083/d0083.html] for more detailed information. If it seems that theft has occurred, call NERDC's director at (352) 392-2061, for assistance.

Protecting Your Password

The CNS Guidebook [http://www.cns.ufl.edu/guidebook/index.html] contains a list of important procedures for protecting your password. We strongly recommend that all users become familiar with this information.

System Access Limitations

After you enter your password correctly, you may still be denied access depending on the following conditions.

Userid Balance  The current funding balance controls how much you can use the system. If the current balance is negative or insufficient to cover the estimated cost of CPU time and output for a job (determined from accounting parameters on the JOBPARM statement), access is denied.

Userid Flags  Certain flags are associated with each userid. Some or all of these flags might be set and you might be denied access. For example, most classroom accounts are limited to those services required for the coursework.

Misuse of Services

You may be subject to severe criminal penalties under the Florida Computer Crimes Act, Chapter 815, Florida Statutes, if you use access numbers, userids, facilities, or data without authorization. A copy of the Computer Crimes Act is reprinted in CNS document D0010 [http://docweb.cns.ufl.edu/docs/d0010/d0010.html] for your convenience. In addition, the University of Florida has an official acceptable use policy [http://www.it.ufl.edu/policies/aupolicy.html] for computer systems. All users of computer systems at UF are responsible for ensuring that their activities are in accord with the provisions of that document.

Your Comments are Welcome

We welcome your comments and suggestions on this and all CNS documentation. Please send your comments to:
UF Computing & Networking Services
112 Bryant Space Sciences Bldg, University of Florida
P.O. Box 112050
Gainesville Florida 32611-2050
(352) 392.2061
<editor@cns.ufl.edu>