

FD42 COMPUTER SYSTEMS – USER REGULATIONS

A risk assessment has just been completed for FD42 computer systems. To maintain our required level of security, the following regulations must be followed by all users of these systems:
MPDNT2 - PAYLOADS - MPD58 - MPDNT5 - PGDEV - PPSWEBDTE - SPICE - MSSNT10 – ROSE - NUTMEG

PASSWORDS

- must not be the same as the user-id and must be more than 8 characters
- must not be dictionary words or dictionary words followed by a digit (most common!)
- must not be related to the name of your company or your project
- must contain at least 1 special character (for example *&%\$#@) NOT just a number
- must not be any part of your name, spouse's name, child's name, pet's name, etc.
- must not be any automobile or sports team name (very common!)
- should contain a combination of uppercase and lowercase letters, as well as numbers and special characters
- should be kept private—no account or password sharing unless authorized

WARNING: A password-cracking tool may be used at any time by the system administrators to ensure that these requirements are being met, and that trivial passwords are not being used.

PUBLIC DOMAIN SOFTWARE

No public domain software is to be installed on any of these systems without the approval of the system manager.

IMPORTANT NOTE TO "PAYLOADS" ACCOUNT HOLDERS

Your username and password MUST NOT BE the same as those on any other system since this system is outside the MSFC firewall and username/passwords are sent in clear text. This policy will allow us to minimize the security threat to other MSFC systems. If your username is the same, notify the system manager. If your password is the same, change it immediately.

TERMINATION OF YOUR ACCOUNT

When you no longer have need of your account, either through the termination of your project or job, you are required to notify the system managers so that your account may be removed.

LOGGING OFF

When you will be away from your workstation, you must either end your session or lock your screen to prevent unauthorized use.

AUDITING

Be aware that your workstation may be audited at any time.

SENSITIVE INFORMATION

IP addresses are considered "security sensitive" information and therefore may not be transmitted through e-mail—exceptions are the IP addresses of public access web servers.

EACH INDIVIDUAL WILL BE HELD ACCOUNTABLE FOR FAILURE TO COMPLY WITH THESE SECURITY REGULATIONS, ALONG WITH ANY DAMAGE WHICH OCCURS AS A RESULT. This will be considered a "security incident" and will be reported to management and IT security personnel.
ANY SUSPECTED UNAUTHORIZED ACTIVITY ON ANY OF THESE SYSTEMS SHOULD BE REPORTED TO THE SYSTEM MANAGERS (DEBBIE GRAHAM 4-3810 OR JOHN JAAP 4-2226) IMMEDIATELY.

These are U.S. Government computers. By accessing and using these systems you are consenting to the monitoring of your keystrokes. Any unauthorized use of these computers may subject you to disciplinary action or even criminal prosecution.

Each user must acknowledge their receipt and understanding of this document by printing it, signing it, and returning it to Debbie Graham, FD42 Computer Security Official; Bldg. 4610—Room 1003.

(name)

(date)