

AUTOMATED INFORMATION SYSTEMS (AIS) SYSTEM USER REQUEST AND ACKNOWLEDGEMENT FORM

This check-in brief outlines basic computer or Automated Information Systems (AIS) security practices that shall be followed while utilizing any Coast Guard owned or operated computer system. There are several controls that you, as a user must be aware of in order to help safeguard against breaches of security. First, the CGSW system is considered to be **SENSITIVE** because it processes Privacy Act protected information (personnel and medical data), financial data (budget, economical and management related information), and mission critical (Coast Guard plans, law enforcement information) type information. Protection of this information is mandated by federal regulations; therefore it is subject to monitoring by authorized personnel to ensure the appropriate security measures remain in effect. **Classified information is not and WILL NOT be processed or stored on the Standard Workstation system! Any instances where classified information is found to be on the system shall be reported immediately to the Area AIS Security Officer (AISSO) or MLCLANT ISSO, and/or your command ISSO. DO NOT delete any documents or messages containing classified information unless directed to do so!** Other important information that you should be aware of is discussed below:

PHYSICAL SECURITY

Physical security and environmental controls shall be used to provide an acceptable level of security to all computers (AIS). Physical security can be achieved through basic measures such as challenging strangers/unknown personnel in your workplace or computer area and by never leaving an active terminal unattended. These are important practices that safeguard against unauthorized use. Logging out when leaving for the day is also required. **Ensure this is always done!** Electrical appliances and magnetic material should not be kept near AIS equipment or storage media (such as floppy diskettes or QIC tapes) because of possible damage/erasure from magnetic fields. Store your floppies and any printouts safely when not in use. Eating, drinking, or smoking near equipment is strictly prohibited.

PASSWORDS

Every user of CGSW systems will use a password. Passwords shall be formulated using A MINIMUM OF 6 (8 for CGSW-III) ALPHANUMERIC CHARACTERS (combination of numbers and letters) to prevent them from being easily guessed. They shall not be names/numbers that can easily be associated with your person (i.e. well known nicknames, spouse's or close relatives (son, daughter, mother, etc.) name, favorite sports teams, type of car you drive, etc.) nor should they be dictionary words (e.g. "SPIDER" or "OFFICE"). Try to choose a password that is easy for you to remember but is not easily guessed. The sharing of passwords is prohibited as is writing it down in easily accessible places (such as "post-it" notes on your desk or in your organizer file under "P", etc.). Remember your password is used to authenticate you and only you as a valid user of the system. Any misuse, abuse, or practices that may jeopardize the system are directly accountable to your user name. If you feel your password has been compromised or that unauthorized personnel are accessing your files, it should immediately be reported to your command ISSO.

ELECTRONIC MAIL

E-Mail is a U.S. Coast Guard owned communications system used to supplement the record message system. It is subject to the same "For Official Use Only" constraints as government mail or telephones, and shall be used to conduct Government business only. Although you may have heard or read about many legal issues concerning expectation of privacy over e-mail, you, as a government employee, should be aware that administrators and technicians have the ability to review e-mail and disseminate it as necessary. With this in mind, understand that **THERE IS NO EXPECTATION OF PRIVACY WHILE USING UNCLASSIFIED COAST GUARD SYSTEMS!**

Additionally, with the availability of gateways to public and private networks (Internet as an example), E-mail transmitted for personal or unauthorized reasons has the potential cause great embarrassment to the Coast Guard. Therefore, Coast Guard resources shall not be used to support private or personal agendas, whether political, moral or philosophical. What this means in that the use of Coast Guard e-mail to address issues such as Government policies, Gay Rights, Abortion, Religion, etc., is, at a minimum, illegal and unethical, and is strictly prohibited. Transmission of messages which contain EFTO (Encrypted For Transmission Only) information (attached documents or forwarded official messages) is not authorized on Coast Guard E-Mail systems. Other information determined to be sensitive (including Privacy Act Information) or For Official Use Only (FOUO) shall not be transmitted via the Internet under any circumstances. EFTO type information shall not be transmitted outside of a Local Area Network (LAN) unless it is contained within an official message. If you have any doubts as to whether the information being transmitted fits into the prohibited category, contact Systems Personnel, your command ISSO or ESU/ESD Personnel.

AUTOMATED INFORMATION SYSTEMS (AIS) SYSTEM USER REQUEST ACKNOWLEDGEMENT FORM

USE OF PERSONALLY OWNED COMPUTERS

Coast Guard Standard Workstation systems and Coast Guard owned/operated PCs are to be used only for conducting official Government business. The use of this equipment for personal reasons or recreation (private letters, games, personal financial gain, etc.) is prohibited. The use of privately owned or leased personal computers or microcomputers to conduct official Government business in a Coast Guard workplace is discouraged, but will be allowed with specific written authorization from the official having command responsibility. Keep in mind that if the PC is authorized for Government work, it must be purged of all Government information prior to being returned to private use. **IT MUST BE INSPECTED** by the AISSO or Security Manager prior to it being returned to private use. **Privately owned PC's must not be used to process classified information!** This prohibition also covers the use of floppy diskettes. Processing classified information on a privately owned PC is a security violation and will result in the entire hard disk of the PC being "wiped" clean in order to declassify it. Incidents must be documented and reported to CGHQ in accordance with chapter 4 of COMDTINST 5510.21 (Information Security Program) and may result in administrative action(s).

COMPUTER VIRUSES/MALICIOUS PROGRAMS (TROJAN HORSES)

Personnel allowed to use privately owned/leased PC's to process Government information shall make every effort to prevent the transmission of computer viruses and Trojan horses through the use of anti-virus software. As a rule, every floppy diskette should be scanned by virus detecting software prior to being placed into a Coast Guard owned/operated PC. If there are Coast Guard owned/operated PC's within your spaces that do not have anti-virus software installed, some of the top software on the market is available from the Area AISSO free of charge.

ILLEGAL SOFTWARE AND GAMES, INTERNET AND BBS

In order to protect the integrity of data on Coast Guard information systems, illegal software ("bootleg" or pirated copies), games, and "public domain" or third party software (shareware) is prohibited. Public domain software may be allowed if it has been certified to perform a necessary function not available through purchased software programs. This use must be documented and authorized by the official having command responsibility for the system. Installation of this type of software must be coordinated through Tiscom with the approved 11-Step justification and the Electronics Systems Support Unit (ESU).

It is illegal to reproduce or copy licensed software (whether Standard Workstation, MS-DOS/Windows, or Macintosh compatible software such as Microsoft Office, Word-Perfect, Excel, Lotus 1-2-3) or any copyright protected software the Coast Guard has purchased. It is also illegal to copy software from personally owned PCs to Coast Guard owned/operated PCs. This practice is illegal and subject to penalty under the law!

Access to the Internet is authorized with CGSW-III, and may be authorized with CGSW-II if the access will benefit performance of the job or enhances information required to complete assigned duties. If authorized access to public bulletin boards or the Internet, games shall not be downloaded! Any software or files downloaded from bulletin boards or the Internet must comply with copyright restrictions and should be scanned for viruses prior to executing on Coast Guard owned/operated systems. As a reminder, access to Internet sites may be monitored by administrators. The use of any Coast Guard own/operated computer to access sites relating to pornography, extreme political views (hate, racism, etc.) or commercial ventures is strictly prohibited and is prosecutable under civil and military law.

GENERAL

Any files within your directory that are no longer necessary should be deleted to prevent your directory from filling up. Conduct this "cleanup" of your directory at least monthly. Files that may be needed for record purposes should be copied to or backed up to floppy disks or QIC tapes. It is the responsibility of each user to ensure he/she receives adequate training in the use of computer systems and the application/programs on it. Training can be accomplished through instruction by someone already familiar with the system or it's applications. Training courses are available through the Electronic Systems Support Unit (ESU). Contact your office's training coordinator for more information.

Problems are an indication that something may be wrong with input, processing, or output operations and should be reported to the technical support trouble desk. Remember, any problem should first be reported to Systems Personnel.

Whenever a problem occurs, immediately write down the error code(s) or message(s) and a description of the work being conducted at the time of the failure.

