Computer Users' Guide For Protecting Information Resources

SEPTEMBER 2002

U.S. DEPARTMENT OF COMMERCE
National Oceanic and Atmospheric Administration
Office of the Chief Information Officer
Information Technology Security Office
1315 East West Highway
Silver Spring, MD 20910

Table of Contents

Section Page

Message

Computer security is more than the protection of sensitive information, it is good management, and the duty of responsible NOAA personnel. We as public servants must protect the materials we handle as a public trust.

I am told that experts in the field of information management agree that most security problems stem from people simply not understanding their responsibilities.

This booklet should be helpful in addressing that problem. It will help all of us within NOAA understand the need for vigilance in handling secure documents and give us the tools for carrying out that mission.

Vice Admiral Conrad C. Lautenbacher, Jr., U.S. Navy (ret.)
Under Secretary of Commerce for Oceans and Atmosphere
and NOAA Administrator

Policy Statement

It is the policy of the National Oceanic and Atmospheric Administration (NOAA) to protect its information resources and allow the use, access, and disclosure of information only in accordance with applicable laws, Federal regulations, and NOAA Directives. This statement reaffirms NOAA's goals for protecting data, information, and its critical infrastructure, the means of processing data.

NOAA's mission to deliver information services to the public and to other government agencies depends critically on the functions of the Information Technology (IT) Security Program. IT security provides the assurance that the computing facilities and the data processed, stored, and distributed from these facilities will be protected to the degree dictated by the sensitivity of the data and as directed by responsible user management and Presidential Decision Directives 62 and 63.

An IT Security Program will be maintained to ensure that cost-effective security controls are set up to protect existing systems, and that such controls are included in the design and development of new systems. These controls will be commensurate with the risks associated with loss of resources and/or services within the NOAA. The term security as defined in this policy, encompasses the full range of physical measures, technological safeguards, and administrative procedures applied to facilities, hardware, software, firmware, data, telecommunications, and personnel.

Goals of the NOAA IT Security Program

- To support NOAA's information services delivery mission and NOAA's business processes.
- To ensure the confidentiality, integrity, and availability of data.
- To protect the critical infrastructure used in the delivery of NOAA products and services.
- To ensure the availability, survivability, and recovery from disaster(s).
- To ensure auditability of all systems.
- To ensure user responsibility for designating the sensitivity of data and for providing and certifying the adequacy of security controls to protect data.
- To ensure management accountability for resources entrusted to users in accomplishing NOAA objectives.
- To ensure **individual accountability** for the data, information, and other computing resources.

Introduction

Today, NOAA computer users develop computer applications and perform other data processing functions that were previously done only by computer operations personnel. As a result, our efficiency and effectiveness are greater, as is our need for data security.

This guide will make you aware of:

- some undesirable things that can happen to data,
- your responsibilities for protecting information technology assets, and
- some practical solutions for reducing your vulnerability to security threats.

Each of us is responsible for protecting data and information resources. Application owners and developers, operators, and users of information systems are **personally responsible** for protecting these resources.

Supervisors must provide appropriate security controls for any information resources entrusted to them. These supervisors are personally responsible for understanding the sensitivity and criticality of their data and the **extent of losses** that could occur if the resources are not protected. Supervisors must ensure that all users of their data and systems are aware of the practices and procedures used to protect the information resources, and ensure that these guidelines are implemented.

If you do not know what your security responsibilities are, **ask your supervisor.**

What Are “Sensitive” Data?

All data are sensitive to some degree; exactly how sensitive is unique to each business environment. Within the Federal Government, personal information is sensitive to **unauthorized disclosure** under the Privacy Act of 1974. Other data are sensitive to fraudulent manipulation for personal gain. For example, systems that process electronic funds transfers, control inventories, issue checks, or control accounts receivables and payables could be exploited, resulting in serious losses. **The integrity and availability of products passed to the public are critical to NOAA’s mission.** Further, inaccurate, incomplete, or obsolete information could result in management decisions that cause serious damage and require time and money to rectify. Data and information that are critical to NOAA’s ability to perform its mission are sensitive to **non-availability.**

One way to determine the sensitivity of data is to ask,

- What will it cost if the data are wrong?
- Manipulated for fraudulent purposes?
- Not available?
- Given to the wrong person?

If the damage is more than you are willing to accept, then the data are sensitive and must be protected by security controls to prevent or lessen the potential loss.

What Risks Are Associated with the Use of Computers?

We rely on computers for virtually all of our major record-keeping functions. This introduces new risks, such as the concentration of tremendous amounts of data in one location. The greater the concentration, the greater the consequences of loss or damage. Another risk is unauthorized access from remote terminals. We must be able to positively identify the user, and ensure that the user is authorized. Newspaper accounts of computer “hackers,” computer virus attacks, and other intruders illustrate the reality of the threat to NOAA computer systems.

What Can NOAA Users Do to Protect Their Assets?

Read this guide to learn about NOAA’s information security objectives, your responsibilities for protecting information technology assets, and ways to achieve that protection. If you have any questions about information security, contact your Information Technology Security Officer (ITSO) using the list on the inside of the back cover.

Reporting Incidents

A security breach is **any violation** of computer security policies, procedures and requirements including misuse, abuse, corruption, unauthorized access, improper disclosure, loss of availability for program operations, or any other compromise of NOAA information resources.

All NOAA employees are to report any security violations to their Line Office ITSO (see contact information at the end of this guide) and to NOAA's Computer Incident Response Team (N-CIRT). An initial **report** must be made **within 24 hours from when the incident is discovered,** and a full written report (using **NOAA Form 47-43**) must be sent to the N-CIRT **within five working days.** You can fill out Form 47-43 from NOAA's Security Web Page: https://www.csp.noaa.gov.

Categories of Incidents on Form 47-43

1. **Malicious Software** - Malicious software includes Trojan Horses, worms, viruses, logic bombs, etc.

2. **IT Security Intrusions**
   a. **Successful Intrusions:**

   - **System Compromise** - System privileges (i.e., root access, accounts with system privileges) are gained by an unauthorized user.
   - **Information Compromise** - Aweakness in the system is exploited that allows data to be manipulated and/or unauthorized access to password files, protected or restricted data, system resources and software/code but does not gain system privileges.
   - **Unauthorized Access** - A valid account is used without permission of the owner.

   b. **Unsuccessful Intrusions** - Monitored attempts at gaining access to NOAA IT assets by unauthorized individuals, that indicate the intent to bypass authentication mechanisms or exploit vulnerabilities in system services, etc.

3. **Denial of Service** - Resources are unavailable for use by the authorized user community.

4. **Hostile Probes/Scans** - The act of using one or more systems to scan targeted systems or networks with intent to conduct or to gather information for unauthorized or illegal activities.

5. **Other IT Security Concerns** - Events that do not fit in other categories or as determined by management (theft of IT resources, damage/sabotage of IT resources).

If you suspect an attack by an intruder, **do not use e-mail** to report the incident; instead, call the **N-CIRT at (301) 713-9111.**

Employees must not discuss actual or suspected incidents with the press.

Password Security

A password is not just a way to get into the computer system; it is a way to keep unauthorized people out. Even though you may not store sensitive material on your computer, your password may be all that a hacker needs to pass from the outer regions (where you compute) to the inner regions (where the sensitive data resides) of your organization's network.

"Password cracking" (guessing a user's password and using it to gain unauthorized access) is a fundamental activity of computer hackers. Password cracking programs can guess an average of 40 percent of all passwords on a computer network. Such a program can be designed to attempt not only all the words in the dictionaries of several languages, but also various permutations of commonly used words.

Since your password is the most vulnerable point of break-in for any would-be hacker, take care to choose and protect that password.

- Passwords must contain at least eight (8) non-blank characters;
- At least one of the characters must be from the alphabet (upper or lower case);
- 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).

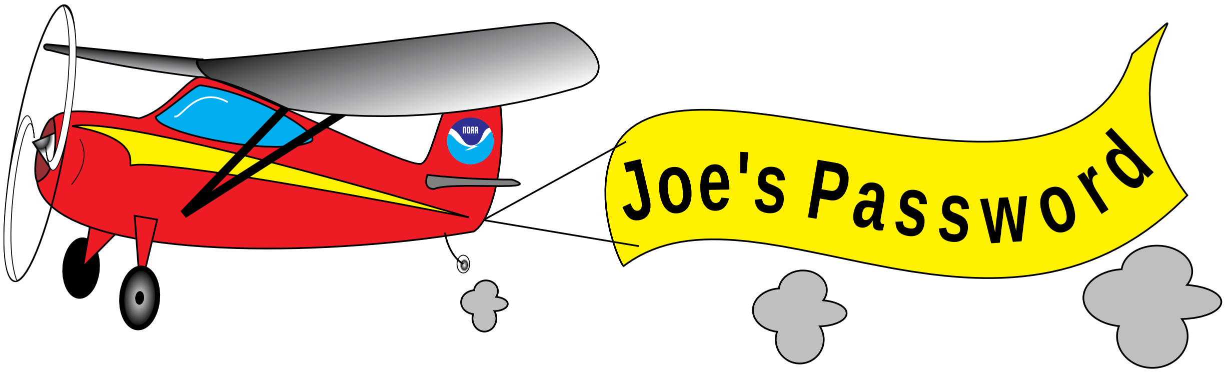
How to Select a Strong Password

Choose a password difficult for a cracker to make educated guesses about (and one that is easy for you to remember). This leaves the hacker no alternative but a brute-force search, trying every possible combination of letters, numbers, and symbols.

Random alphanumeric compositions (for example, AX$78BO@) are difficult to guess, but can be hard to remember.

Some ideas for constructing a strong password include:

- Use an acronym from an easy to remember phrase. "The Cat in the Hat Ate Green Eggs" can translate into "TCITH8GE."
- Alternate between one or two consonants and one or two vowels. This provides nonsense words that are usually pronounceable, and thus easily remembered. Examples: Aroutboo, Aquadpop.
- Choose two short words and concatenate them with a punctuation character between them. For example: Adog;rain, Abook+mug, Akid?goat.



- Use both upper and lowercase letters.

- Use numbers and special symbols (!@#$) with letters. For example, “You Are My Sunshine” could become “Yr#M#ss.”

- Use misspelled words (kantUSpel?).

Do Not Use

- Any example used in the previous section or in a similar discussion of passwords.

- Your login name in any form (as-is, reversed, capitalized, doubled, etc.).

- A name associated with you in any way (your middle initial, spouse’s first name, a maiden name, pet’s name, child’s name, or favorite celebrity, sports team, or hobby).

- Any proper name (first name or last name).

- Other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the brand of your automobile, the name of the street you live on, etc.

- Any word in any dictionary in any language in any form, spelled forward or backward.

- Slang words, obscenities, technical terms, jargon, or computer brand names.

- Simple patterns, including: passwords of all the same letters or digits, simple keyboard patterns (e.g., 12345, GHIJK, 2468), or anything that someone might easily recognize if they see you typing it.

- Objects that are in your field of vision at your workstation.

- Any password that you have used in the past or any password with less than eight characters.

Changing Passwords

Passwords must be changed every 90 days. Change your password immediately if you suspect that it has been compromised. Terminate user accounts when the password owner transfers or leaves NOAA employment.

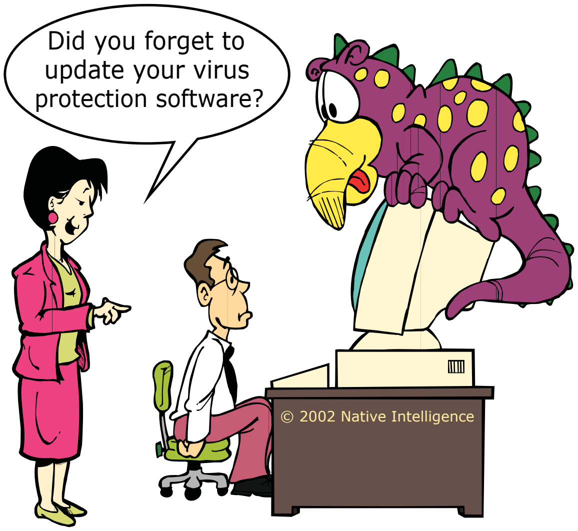
Why Go Through All The Trouble?

Passwords are the primary defense and front-line security for your data. If someone obtains your password, they have complete access to your account, your data, and to **all the system privileges you have.** You must not share your password because **you are responsible for all actions taken by anyone with whom you share your password.**

To Protect Your Password

- Ensure that only you know your password.
- Ensure that your password can not be easily guessed by a password cracker.
- Change your password every 90 days.
- Use a minimum of eight characters. Generally, the longer the password, the more secure it is.
- Never write your password down anywhere, or tape it near a calendar or terminal.
- Report any known or suspected compromises of your passwords.
- Change your password immediately if it has been compromised or if it is found to be non-compliant with NOAA policies.

Malicious Software


Did you forget to update your virus protection software?
© 2002 Native Intelligence

Malicious software includes viruses and other destructive programs, such as Trojan Horses and network worms. This type of software is often written as an independent program that appears to provide a useful function, but contains destructive code. It can spread quickly though software "bulletin boards;" shareware; and users unaware of the danger, who copy and share these programs. Networks are particularly vulnerable as they allow rapid spread of a virus to systems connected to the network.

A program infected with a virus can infect any host in which the program is used, and any user may become an unwitting propagator. NOAA's dependence on networked computer systems, personal computers (PCs), and office automation makes us susceptible to viruses.

Most of NOAA's Line Offices have been infected with computer viruses. In many cases, data was not lost, but time and staff resources were spent tracking and eliminating these viruses. These viruses are unintentionally received through diskettes, bulletin boards, on-line services, e-mail, the Internet, and organizational networks.

To minimize the risks to NOAA systems and networks, all employees should:

- Ensure that all PC machine-readable media are scanned for malicious software before initial use. This includes software sealed in "shrink-wrapped" plastic.

- Use only authorized software and data obtained from reliable sources. Viruses are often spread through free or shared programs, games, and demonstration programs. Employees must not use privately-owned software or take software from their office without management approval. Commercial software must be obtained through appropriate procurement channels.

- Obtain management approval before using shareware and freeware. Software obtained electronically from bulletin boards and the Internet should be downloaded to newly formatted diskettes and scanned for viruses before being transferred to the computer hard disk. All newly acquired software, regardless of source, is subject to the scanning requirements.

- Scan all out-going and incoming software and data diskettes for viruses or other malicious coding. Use only new media for making copies for distribution. Where possible, use a stand-alone computer system when preparing copies for distribution.

- Back up software and data often and write-protect original diskettes before making back-up copies. If a virus destroys the working copy, the original software is still available.

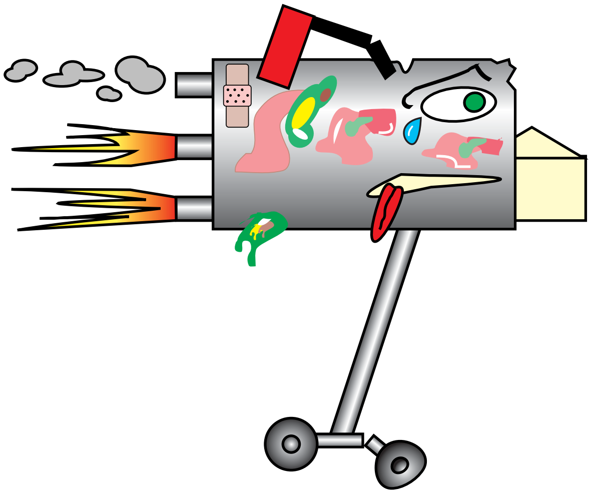
- Use only new or freshly-formatted diskettes for copying software for back-up storage. Used disks may already contain malicious programs which would contaminate the back-up copies.

- Ensure that portable computer systems, such as laptops, that leave NOAA-controlled areas are scanned for viruses before and after connecting to systems or software owned by other organizations.

- Never use a local area network file server as a workstation. File servers should be located in areas where access is restricted during working hours and locked after hours.

- Only start up (boot) your computer from the original write-protected system master or a trusted copy.

E-mail Viruses



Viruses can be spread through a user's reading of e-mail.

Recent methods exploit the programs used to read e-mail. These attacks can use macro languages to cause programs on the reader's system to spread the infected e-mail to other systems, as was the case with the Melissa virus.

Be wary of file attachments that are not expected or are from strangers. Delete such attachments or save them and then check them for viruses before running them.

Virus Protection

To protect your software and data, use NOAA's standard detection software, McAfee. This software is capable of continuous monitoring and reporting malicious programs and is required to be installed on every NOAA PC to prevent contamination.

NOAA users can obtain copies for home and office PCs by contacting their system administrator or Line Office ITSO. (See inside back cover for the ITSO list.) The software can also be downloaded from the NOAA Security Home Page: **https://www.csp.noaa.gov/.**

Viruses also spread through floppy disks, so isolating yourself from online services and the Internet will not protect your system from viruses.

NOAA Guidelines for Dealing with E-mail Spam

Spam (aka UCE: Unsolicited Commercial E-Mail) is the Internet version of "Junk E-Mail." It is an attempt to deliver a message, over the Internet, to someone who would not otherwise choose to receive it. Almost all spam is commercial advertising. Potential target lists are created by scanning Usenet postings, stealing Internet mailing lists, or searching the Web for addresses. Such information is gathered with automated searches to retrieve E-Mail addresses for spamming.

The low cost of E-Mail spamming engines offered for sale with millions of E-Mail addresses, coupled with the fact that the sender does not pay extra to send E-Mail, has resulted in the current explosive growth of "junk E-Mail." Currently, unless the spammer offers to sell illegal items, there is no legal remedy to use to stop E-Mail spammers.

Several bills have been introduced in Congress to deal with this problem.
For information on their status, go to: **http://www.cauce.org/**.

If you receive mail in your NOAA mailbox, there are varying ways to deal with it.
The easiest and most obvious is to **simply delete it**.

If, however, you feel that the message refers to something illegal or offensive (pornography), or you find it threatening, please notify your local IT security contact and/or email administrator. Either they or you should then forward it to **abuse@noaa.gov**. Also, if the spam asks you to open a bank account to deposit large sums of money usually associated with an oil deal and/or the Nigerian or other government, you must report it. For more information, see: **http://www.secretservice.gov/alert419.shtml**.

When sending these messages, **always** include complete mail headers. The complete header information **must** be included since the return address almost never reflects the sender's identity. Instructions for doing this with Netscape Messenger are:

To forward messages with complete SMTP headers from Netscape Messenger:
This is best done by forwarding messages “Inline.” In Netscape Communicator/Messenger, choose “Headers” and “All” from the “View” Menu. Then, click on and hold the “Forward” button. A dropdown menu will appear. Drag the cursor to “Inline” and choose it.

Instead of clicking on the Forward button, you can also right-click the message you want to forward to **abuse@noaa.gov**. A menu will appear, and you can choose “Forward Inline.” Messages formatted like this can easily be cut and pasted into new messages by the abuse team to be sent to Service Providers.

DO NOT TRY TO DEAL WITH THE SPAM YOURSELF

- DO NOT reply to the spammer. The sender address is almost always not an actual address. If it is a working address, the spammer may be using it to simply verify that your email address is valid.
- For the same reason, DO NOT follow instructions in the spam for getting yourself “removed” from their list. This includes sending a message to another address or going to a “removal” website.
- DO NOT use spam reporting services outside of NOAA (such as “spamcop”). These services are easily misused, and NOAA employees have accidentally implicated NOAA servers in spamming, thus submitting those servers for consideration to blacklisting databases.
- DO NOT spam, mail bomb, or hack spammers. In many cases the site indicated as the source of the spamming is not the spammers real site, so attacking that site is not only wrong, but you are actually “spamming” yourself.
- DO NOT go to websites that the spammer may be advertising. Alot of information can be gathered by web sites, not to mention the fact that the sites may actually contain malicous code that could damage your computer.

While NOAA has the capability to filter messages as they come in from the Internet, spam is extremely hard to block. No matter what anti-spam websites say, it’s impractical to scan for phrases or addresses that are used in messages, or servers that may be used to send spam, since these can easily be changed. Efforts have been made to create huge blacklists of servers known to be used for spam distribution, but many of these servers have been used without the owner’s permission, and may actually have legitimate reasons to send email into NOAA.

Spammers usually expect to send out messages until they get caught; when that happens, they simply move on to another ISP and find another server to distribute their messages.

Computer Virus Hoaxes

The Internet is a source of information about computer virus threats. Interspersed among real virus notices are computer virus hoaxes. Virus hoaxes are sometimes called Junk-mail viruses because they act like other computer viruses, only they use people as the method of infecting new systems. While these hoaxes do not infect systems, they are time consuming and costly to handle.

What to Do When You Receive a Virus Warning

1. Do not forward the warning to co-workers and/or friends
2. Forward the message to your system administrator to validate first
3. Keep informed, read about viruses and hoaxes at the following sites:

   Computer Virus Myths
   http://www.kumite.com/myths/

   Network Associates Virus Hoax Center
   http://www.nai.com/asp_set/anti_virus/library/hoaxes.asp

4. Be aware that warnings without the name of the person sending the original notice, or warnings with names, addresses and phone numbers that do not actually exist are probably hoaxes.

A warning that urges you to pass it on to your friends should raise a red flag that the warning may be a hoax. The more urgent the message sounds, the more skeptical you should be.

A virus hoax listing can be viewed at: http://vil.nai.com/VIL/hoaxes.asp.

The Internet

Internet Use Policy. NOAA follows the Department of Commerce (DOC) Internet Use Policy. Provided below are statements that reflect official guidance on Departmental use of the Internet and e-mail services. The full text of the policy can be viewed at:
http://www.doc.gov/cio/oipr/ITSec/internetpolicy1.htm

It is the policy of the Department to allow and encourage the use of Internet services to support the accomplishment of the various missions. Use of the Internet requires responsible judgement, supervisory discretion and compliance with applicable laws and regulations. Users must be aware of information technology security and other privacy concerns. Users must also be aware of and follow management directives for Internet usage.

Internet services provided by the Department, like other Government equipment and resources, are to be used only for authorized purposes. The Department recognizes that it is in the interest of the Government that personnel become proficient and maintain proficiency in using the Internet. To this end, the restrictions outlined below regarding Internet use during official working hours and non-working hours should be followed by Department personnel when using Internet services provided by the Department.

1. Internet services provided by the Department during official working hours are to be used for authorized purposes only. This may include using Internet services to train personnel on using the Internet, provided prior approval is obtained from an employee's supervisor.

2. Internet service represents a corporate resource that must be managed in an efficient and cost effective manner.

3. Internet access should be achieved using standard and commonly available tools, unless a specific requirement calls for a unique approach.

4. Operating Units should ensure that their presence on the Internet fulfills mission requirements in a professional manner. Information made available via the Internet should be accurate, relevant, up-to-date, and professionally presented.

5. Operating Units and Departmental offices may use the Internet to exchange information with the public and internally as an information technology tool. It is to be considered as one of a number of tools and an alternative commercial communication network that is available to DOC.

6. Information technology security requirements shall be a primary consideration in the decision process leading to the use of the Internet. Operating Unit offices must take adequate precautions when processing data or storing data on computers connected to the Internet and when transmitting data on or through the Internet. Certification and accreditation requirements for all sensitive and classified general support and major application systems apply to use of the Internet for processing or transmitting sensitive or classified data.

7. Unless prohibited by the specific policies of the employee's bureau/Operating Unit, the use of Internet services and e-mail provided by the Department during non-working hours is not limited to official purposes only. This policy will assist employees in becoming proficient in using the Internet and will enhance their professional development at minimum expense to the Government. However, personnel may not use government printers or supplies in conjunction with personal Internet and e-mail activities. Activities for which Department Internet and e-mail services may not be used, during working or non-working hours, include the following:

   - the pursuit of private commercial business activities or profit-making ventures (i.e., employees may not operate a business with the use of the Department's computers and Internet resources);
   - matters directed toward the success or failure of a political party, candidate for partisan political office, or partisan political group;
   - prohibited direct or indirect lobbying;
   - use of Internet sites that result in an additional charge to the Government;
   - engaging in prohibited discriminatory conduct;
   - the obtaining or viewing of sexually explicit material;
   - any activity that would bring discredit on the Department; or any violation of statute or regulation.

   The Department expects personnel to conduct themselves professionally while using Department resources. Personnel must refrain from using Department resources for activities that are disruptive to the work place or in violation of public trust.

   Like all other Government computer use, use of Government equipment for personal use of the Internet may be monitored and recorded. Anyone using Government equipment consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity or employee misconduct, system personnel may provide the evidence of such monitoring to Department and law enforcement officials. Individuals are not guaranteed privacy while using government computers and should, therefore, not expect it. To the extent that employees wish that their private activities remain private, they should avoid using the Department's Internet or e-mail for such activities.

8. Unless prohibited by the specific policies of the employee's bureau/Operating Unit, limited personal use of e-mail during duty hours is permissible, as such use will help promote proficiency in electronic communications, including use of the Internet, and provides an alternative method for authorized personnel communications, which will promote Government efficiency.

   At no time may Government e-mail addresses be used in a manner which will give the impression that an otherwise personal communication is authorized by the Department.

   Personal use of e-mail cannot interfere with the official business of the employee or organization, such as spending an inappropriate amount of time during duty hours (e.g., sending more than four brief messages per day), filling up a mailbox with personal messages so as to prevent official messages from being delivered, or disseminating chain letters.

Netiquette

Internet tips on proper “Netiquette.”

Search for the FAQs: Frequently Asked Questions (FAQs) are available throughout the World Wide Web (WWW).

Don’t flame: Remember the old adage about “never start something, unless you’re prepared to finish it”? Well, in regard to flaming, it would read more like “never start something unless you’re prepared for it to never finish.” Before you ignite the first match in a flame war, ask yourself if you’re willing to endure the return fire.

Don’t SHOUT: Using ALL CAPS in Net correspondence implies that you are SHOUTING.

Observe before joining in: If you sign onto news groups or mailing lists, read the postings for at least a few days, until you know what list participants talk about.

Stay on the topic: If you observe before posting, you’ll notice that those maintaining the list or groups usually try to stay on topic. You should do the same.

Take a breath or two before you respond: E-mail correspondence can not be unsent. Keep your communications professional.

Release the communications line when you’re finished.

Use emoticons: The nuances of human interaction (the glance, wink, smirk, sigh) are absent in electronic communications (other than video-conferencing). Emoticons help avoid misunderstandings. Samples include:

:-) (Happy)

:-((Unhappy)

:-C (Very unhappy)

:-} (Smirk)

:-J (Tongue-in-cheek)

:X (Oops!)

<L> (Laughing)

<G> (Grinning)

Proper Use of Government Equipment

When Should We Turn Equipment Off?

Over time, the personal computers and associated equipment which are used in the Federal workforce are being replaced with equipment that automatically “powers down” when not in use. To further reduce the consumption of energy:

1. Turn equipment off during non-work hours. The energy consumption of a personal computer can be reduced by more than 75 percent by turning off the machine during non-work hours.
2. Turn equipment off whenever you leave the office for an extended period of time or for any long period of inactivity when it will not be inconvenient to re-boot or re-start.
3. Turn off just the monitor between shorter absences of use. This will reduce the unit’s power consumption about 50 percent.

Equipment / Information That Is No Longer Needed

Before disposing of any storage media, your ITSO must ensure that overwriting the media erases all software and information with release restrictions. Current Federal regulations permit giving surplus IT equipment to organizations outside the NOAA community. Other organizations are not authorized to possess copyrighted software licensed to NOAA or restricted information (that is, information whose distribution is controlled) that may be stored on NOAA’s surplus media. Releasing copyrighted software or restricted information outside of NOAA, even accidentally, may expose the responsible ITSO and the Government to considerable liability. Media that do not permit overwriting should be destroyed or transferred to another authorized user within NOAA.

If you have any questions concerning releasing information, data, or software on obsolete storage media, erase the media before releasing them for disposal.

> **Note:** Deleting information and erasing information are very different. Deleting usually removes only pointers to the files that contain the information. The information remains on the medium and may often be recovered using widely available software tools. Erasing overwrites the data fields so that the information is truly gone.

Software Security

The Law

Title 17, United States Code, Section 106 gives copyright owners exclusive rights to reproduce and distribute their material, and Section 504 states that individuals found infringing on copyright can be held liable for damages to the copyright owner. Title 18, United States Code provides felony penalties for software copyright infringement.

NOAA employees are responsible for assuring that commercial software acquired by the Government is used only in accordance with licensing agreements. It is also your responsibility to assure that any proprietary software is properly licensed before being installed on government equipment. This policy does not apply to software developed by or for a Federal agency where no restrictions apply to its use or distribution within the Federal government.

Your acquisition and use of software is governed by copyright law and the license agreement accompanying the software. Therefore, you should be aware:

> ***It is illegal*** to copy or distribute software or its accompanying documentation, programs, applications, data, codes, and manuals, without permission or a license from the copyright owner.
>
> ***It is illegal*** for organizations to consciously or unconsciously encourage, allow, compel, or pressure employees to make or distribute unauthorized software copies.
>
> ***It is illegal*** to infringe the laws against unauthorized software copying because someone requests or compels it.
>
> ***It is illegal*** to lend software so that a copy can be made.
>
> ***It is illegal*** to make, import, possess, or deal with articles intended to facilitate the removal of any technical means applied to protect the software program.

The Language

Here are some definitions of commonly used terms about the management and use of original software under copyright law:

Intellectual Property — An original computer program is regarded by law as the intellectual property of the person or company who created the work. Computer programs are protected under copyright law, which provides that any unauthorized copying of such works is illegal.

Software License Agreement — A “Software License Agreement” states the terms of usage, as permitted by the copyright owner, for the specific software product to which it pertains. The license agreement accompanying software is stated explicitly in the software documentation or on the computer screen when the program is started. The price of software covers the legal acquisition of the software license and binds the purchaser to use the software only according to the terms and conditions stated in the license.

Unauthorized Copying — Unless otherwise stated, the purchase of a software license allows the purchaser to make only one “back-up” copy, to be used in case the original software disk malfunctions or is destroyed. Any other copy of the original software is considered to be an unauthorized copy, and is an infringement of the license agreement and the copyright law, which protects software and governs its use.

Software Piracy — Software piracy is the term used to describe the unauthorized copying or use of a computer program in any manner other than what is permitted by copyright law or by the author as stated in the software license agreement. Any person who engages in software piracy commits an illegal act under general copyright law.

The Code of Ethics

Any duplication of licensed software except for backup and archival purposes is a violation of the law. Any unauthorized duplication of copyrighted computer software is contrary to the NOAA’s standards of conduct. In compliance with NOAA’s software license agreements and NOAA’s policy concerning software duplication, an employee:

1. Will use all software in accordance with our license agreements.

2. Will be provided legitimate software. No employee of NOAA will make any unauthorized copies of any software under any circumstances. Anyone found copying software other than for backup purposes violates the law.

3. Will not tolerate the use of any unauthorized copies of software in NOAA. Any person illegally reproducing software can be subject to civil and criminal penalties including fines and imprisonment. We do not condone illegal copying of software under any circumstances and anyone who makes, uses, or otherwise acquires unauthorized software shall be appropriately disciplined.

4. Will not give software to any outsiders (including clients, customers, friends, and others).

5. Who determines that there may be a misuse of software within NOAA will notify his or her supervisor or ITSO (see contact information at the end of this guide).

6. Will ensure that all software used on NOAA computers will be properly purchased through appropriate procedures.

Rules of Behavior

NOAA employees and contractors are individually responsible for the protection and security of data, software, and hardware assigned to, or used by them, and all forms of information technology, including voice mail and faxes.

The following rules of behavior are for all NOAA Information Technology (IT) systems users. At a minimum, violations will result in loss of access privileges and/or written reprimands. Copyright or Privacy Act breaches can result in fines up to $50,000, imprisonment, and loss of employment. These requirements also apply to volunteers, contract staff, and other individuals who are not NOAA employees but to whom the agency grants access to use NOAA equipment/software.

NOAA's Information Technology Systems Rules of Behavior for All Users

1. PASSWORDS:
   a. Do not share!
   b. Do not accept another user's password, even if offered
   c. Use unique passwords:
      (1) 8 to 20 characters long
      (2) mix of symbols, numbers, and letters (upper and lower case)
   d. Change to a new password every 90 days or sooner

2. POLICY:
   a. IT equipment is for official Government business only
   b. Chain letters, games, union announcements, and threatening, obscene, or harassing messages are not allowed
   c. Use of broadcast feature must be approved by management
   d. Warning banners are to be installed and displayed when users connect to a system and are prompted for login information

3. PROCEDURES:
   a. Do not reconfigure equipment, software, or access unless operating under an approved and applicable standard procedure
   b. Protect passwords, information, equipment, systems, networks, and communications pathways to which you have access:
      (1) Report anything unusual or suspicious (especially viruses) to your supervisor or Information Technology Security Officer (ITSO)
      (2) Never leave your terminal without logging off
      (3) Minimize the threat of viruses:
         (a) Write-protect diskettes
         (b) Virus check any "foreign" data source
         (c) Never circumvent the anti-virus safeguards on the system

NOAA’s Information Technology Systems Rules of Behavior for All Users - Continued

4. PERSONAL RESPONSIBILITY:
   a. Realize that these “Rules of Behavior” apply even if you don’t take time to read them Violations will result in loss of access and/or written reprimands, fines, imprisonment, and loss of employment
   b. Comply with copyright and site licenses of proprietary software. No personally purchased software is allowed on Government equipment
   c. Notify IT manager if access to resources is beyond what you need
   d. Attend mandatory security awareness and information protection training
   e. Users will be held accountable for their actions on NOAA systems

5. PRIVACY:
   a. Protect employee information, medical records, historical data or client lists
   b. Properly dispose of unneeded data:
      (1) Don’t throw sensitive hard copy into a wastebasket (shred or burn)
      (2) Delete sensitive information from storage on hard drive and diskettes permanently by overwriting; ask your ITSO for aid in doing this, if necessary

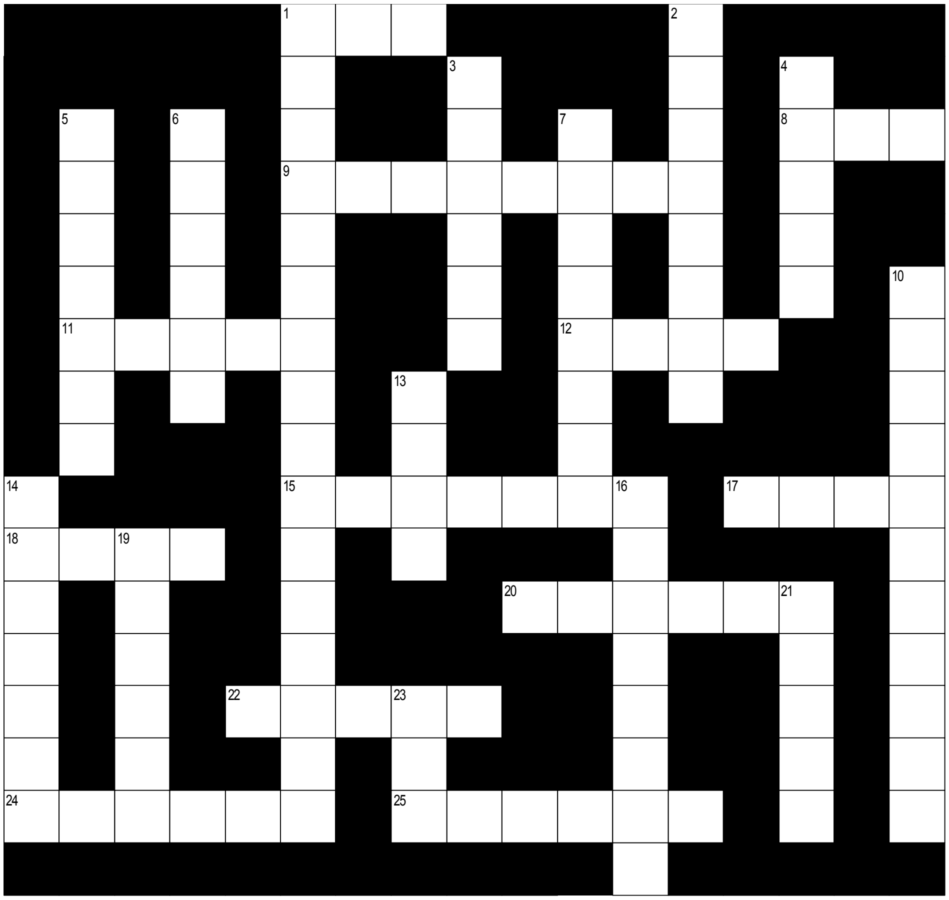
Security Unscramble Game

Unscramble the third letter of each word in the list below to uncover an important phrase.

water
tsunami
hackers
virus
access
countermeasure
data
physical
memory
assets
theft
program
crime
agent
terrorist
application

See page 24 for the answer.

Security Crossword Puzzle



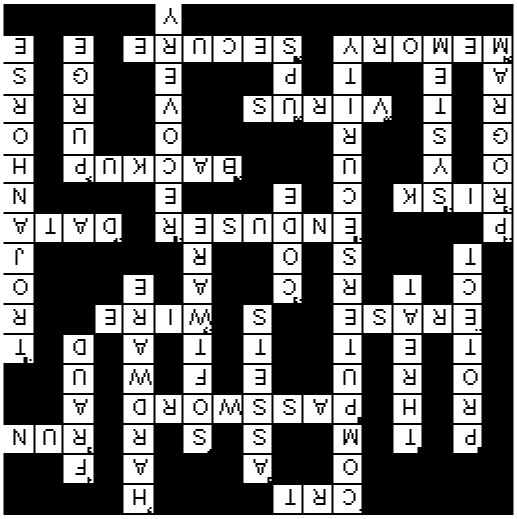
ACROSS

1	Monitor
8	Execute
9	Protected word
11	Degauss
12	Electronic Intruder
15	Operator
17	Information
18	Cost
20	Download
22	Threat
24	Storage
25	Lock

DOWN

1	Awareness of (2 words)
2	CPU
3	Software, hardware, data
4	Deception
5	Make Safe
6	Danger
7	WordPerfect
10	"Beware of hackers bearing gifts" (2 words)
13	Password
14	Sequence of Instructions
16	Backup Utility Function
19	Interacting elements
21	To remove
23	Uninterupted power supply

Crossword Puzzle Solution



Answer to word scramble:

COMPUTERSECURITY

Information Technology Security Officers (ITSOs)

NOAA Chief Information Officer - Carl Staton
Director of Information Technology Security Office - Becky Vasvary Gaujot

This list of the ITSOs is maintained on the security web site: https://www.csp.noaa.gov/

Line Office	Name	Email Address	Telephone Number
NOAA	Conrad Lovley Alternate - Linda Laboskie	Conrad.Lovley@noaa.gov Linda.D.Laboskie@noaa.gov	(301) 713-0042 x 218 (301) 713-0042 x 194
OFA	Joseph C. Smith, III	Joseph.C.Smith.III@noaa.gov	(301) 763-6300 x 141
NOS	John D. Parker Alternate - Thomas K. Murphy	John.D.Parker@noaa.gov Thomas.K.Murphy@noaa.gov	(301) 713-1156 x 174 (301) 713-1156 x 102
NWS	William Carter Alternate - Gerald Singleton	William.Carter@noaa.gov Gerald.Singleton@noaa.gov	(301) 713-1360 x 118 (301) 713-0864 x 153
OAR	Sandra Wine Alternate - Jeremy Warren	Sandra.J.Wine@noaa.gov Jeremy.Warren@noaa.gov	(301) 713-9040 x 127 (301) 713-9040 x 169
NMFS	Ron Trenti Alternate - Bill Bradley	Ron.Trenti@noaa.gov Bill.Bradley@noaa.gov	(301) 713-2372 x 184 (301) 713-2372 x 175
OMAO	Greg Bass	Gregory.Bass@noaa.gov	(301) 713-3425 x 179
NESDIS	Charles MacFarland Alternate - George Saxton	Charles.MacFarland@noaa.gov George.Saxton@noaa.gov	(301) 713-0574 x 157 (301) 713-1315