NIST Special Publication 500-171

Computer
Systems
Technology

S DEPARTMENT OF
OMMERCE
ational Institute of
andards and
echnology

NIST



# Computer User's Guide to the Protection of Information Resources

Cheryl Helsing
Marianne Swanson
Mary Anne Todd

The National Institute of Standards and Technology[1] was established by an act of Congress on March 3, 1901. The Institute's overall goal is to strengthen and advance the Nation's science and technology and facilitate their effective application for public benefit. To this end, the Institute conducts research to assure international competitiveness and leadership of U.S. industry, science and technology. NIST work involves development and transfer of measurements, standards and related science and technology, in support of continually improving U.S. productivity, product quality and reliability, innovation and underlying science and engineering. The Institute's technical work is performed by the National Measurement Laboratory, the National Engineering Laboratory, the National Computer Systems Laboratory, and the Institute for Materials Science and Engineering.

## *The National Measurement Laboratory*

Provides the national system of physical and chemical measurement; coordinates the system with measurement systems of other nations and furnishes essential services leading to accurate and uniform physical and chemical measurement throughout the Nation's scientific community, industry, and commerce; provides advisory and research services to other Government agencies; conducts physical and chemical research; develops, produces, and distributes Standard Reference Materials; provides calibration services; and manages the National Standard Reference Data System. The Laboratory consists of the following centers:

- Basic Standards[2]
- Radiation Research
- Chemical Physics
- Analytical Chemistry

## *The National Engineering Laboratory*

Provides technology and technical services to the public and private sectors to address national needs and to solve national problems; conducts research in engineering and applied science in support of these efforts; builds and maintains competence in the necessary disciplines required to carry out this research and technical service; develops engineering data and measurement capabilities; provides engineering measurement traceability services; develops test methods and proposes engineering standards and code changes; develops and proposes new engineering practices; and develops and improves mechanisms to transfer results of its research to the ultimate user. The Laboratory consists of the following centers:

- Computing and Applied Mathematics
- Electronics and Electrical Engineering[2]
- Manufacturing Engineering
- Building Technology
- Fire Research
- Chemical Engineering[3]

## *The National Computer Systems Laboratory*

Conducts research and provides scientific and technical services to aid Federal agencies in the selection, acquisition, application, and use of computer technology to improve effectiveness and economy in Government operations in accordance with Public Law 89-306 (40 U.S.C. 759), relevant Executive Orders, and other directives; carries out this mission by managing the Federal Information Processing Standards Program, developing Federal ADP standards guidelines, and managing Federal participation in ADP voluntary standardization activities; provides scientific and technological advisory services and assistance to Federal agencies; and provides the technical foundation for computer-related policies of the Federal Government. The Laboratory consists of the following divisions:

- Information Systems Engineering
- Systems and Software Technology
- Computer Security
- Systems and Network Architecture
- Advanced Systems

## *The Institute for Materials Science and Engineering*

Conducts research and provides measurements, data, standards, reference materials, quantitative understanding and other technical information fundamental to the processing, structure, properties and performance of materials; addresses the scientific basis for new advanced materials technologies; plans research around cross-cutting scientific themes such as nondestructive evaluation and phase diagram development; oversees Institute-wide technical programs in nuclear reactor radiation research and nondestructive evaluation; and broadly disseminates generic technical information resulting from its programs. The Institute consists of the following divisions:

- Ceramics
- Fracture and Deformation[3]
- Polymers
- Metallurgy
- Reactor Radiation

[1]Headquarters and Laboratories at Gaithersburg, MD, unless otherwise noted; mailing address Gaithersburg, MD 20899.
[2]Some divisions within the center are located at Boulder, CO 80303.
[3] Located at Boulder, CO, with some elements at Gaithersburg, MD.

NIST Special Publication 500-171

# Computer User's Guide to the Protection of Information Resources



Cheryl Helsing
Deloitte, Haskins & Sells

Marianne Swanson
Mary Anne Todd

National Computer Systems Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899

October 1989


U.S. DEPARTMENT OF COMMERCE
**Robert A. Mosbacher, Secretary**
NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
Raymond G. Kammer, Acting Director

NIST

## Reports on Computer Systems Technology

The National Institute of Standards and Technology (NIST) (formerly the National Bureau of Standards) has a unique responsibility for computer systems technology within the Federal government. NIST's National Computer Systems Laboratory (NCSL) develops standards and guidelines, provides technical assistance, and conducts research for computers and related telecommunications systems to achieve more effective utilization of Federal information technology resources. NCSL's responsibilities include development of technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive unclassified information processed in Federal computers. NCSL assists agencies in developing security plans and in improving computer security awareness training. This Special Publication 500 series reports NCSL research and guidelines to Federal agencies as well as to organizations in industry, government, and academia.

**Library of Congress Catalog Card Number: 89-600764**
**National Institute of Standards and Technology Special Publication 500-171**
**Natl. Inst. Stand. Technol. Spec. Publ. 500-171, 16 pages (Oct. 1989)**
**CODEN: NSPUE2**

**U.S. GOVERNMENT PRINTING OFFICE**
**WASHINGTON: 1989**

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402

The National Institute of Standards and Technology (NIST) is responsible for developing standards, providing technical assistance, and conducting research for computers and related systems. These activities provide technical support to government and industry in the effective, safe, and economical use of computers. With the passage of the Computer Security Act of 1987 (P.L. 100-235), NIST's activities also include the development of standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems. This guide is just one of three brochures designed for a specific audience. The "Executive Guide to the Protection of Information Resources," and the "Managers Guide to the Protection of Information Resources" complete the series.

## ACKNOWLEDGMENTS

This guide was written by Cheryl Helsing of Deloitte, Haskins & Sells in conjunction with Marianne Swanson and Mary Anne Todd of the National Institute of Standards and Technology.

# Introduction

Today's computer technology, with microcomputers and on-line access, has placed the power of the computer where it belongs, **in YOUR hands. YOU, the users,** develop computer applications and perform other data processing functions which previously were only done by the computer operations personnel. These advances have greatly improved our efficiency and effectiveness but, also present a serious challenge in achieving adequate data security.

While excellent progress has been made in computer technology, very little has been done to inform users of the vulnerability of data and information to such threats as unauthorized modification, disclosure, and destruction, either deliberate or accidental. This guide will make you aware of some of the undesirable things that can happen to data and will provide some practical solutions for reducing your risks to these threats.

## WHO IS RESPONSIBLE FOR PROTECTING DATA AND INFORMATION?

The statement that "security is everyone's responsibility" is absolutely true. Owners, developers, operators and users of information systems each has a personal responsibility to protect these resources. Functional managers have the responsibility to provide appropriate security controls for any information resources entrusted to them. These managers 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. Managers must ensure that all users of their data and systems are made aware of the practices and procedures used to protect the information resources. When you don't know what your security responsibilities are, **ASK YOUR MANAGER OR SUPERVISOR.**

## WHAT IS "SENSITIVE" DATA?

All data is 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. In some cases, data is far more sensitive to accidental errors or omissions that compromise accuracy, integrity, or availability. For example, in a Management Information System, inaccurate, incomplete, or obsolete information can result in erroneous management decisions which could cause serious damage and require time and money to rectify. Data and information which are critical to an agency's ability to perform its mission are sensitive to nonavailability.

Still other data are sensitive to fraudulent manipulation for personal gain. Systems that process electronic funds transfers, control inventories, issue checks, control accounts receivables and payables, etc., can be fraudulently exploited resulting in serious losses to an agency.

One way to determine the sensitivity of data is to ask the questions "What will it cost if the data is wrong? Manipulated for fraudulent purposes? Not available? Given to the wrong person?" If the damage is more than you can tolerate, then the data is sensitive and should have adequate security controls to prevent or lessen the potential loss.

## WHAT RISKS ARE ASSOCIATED WITH THE USE OF COMPUTERS?

Over the past several decades, computers have taken over virtually all of our major record-keeping functions. Recently, personal computers have made it cost-effective to automate many office functions. Computerization has many advantages and is here to stay; however, automated systems introduce new risks, and we should take steps to control those risks.

We should be concerned with the same risks that existed when manual procedures were used, as well as some new risks created by the unique nature of computers themselves. One risk introduced by computers is the concentration of tremendous amounts of data in one location. The greater the concentration, the greater the consequences of loss or damage. Another example is that computer users access information from remote terminals. We must be able to positively identify the user, as well as ensure that the user is only able to access information and functions that have been authorized. Newspaper accounts of computer "hackers," computer virus attacks,

and other types of intruders underscore the reality of the threat to government and commercial computer systems.

## HOW MUCH SECURITY IS ENOUGH?

No matter how many controls or safeguards we use, we can never achieve total security. We can, however, decrease the risk in proportion to the strength of the protective measures. The degree of protection is based on the value of the information; in other words, how serious would be the consequences if a certain type of information were to be wrongfully changed, disclosed, delayed, or destroyed?

# General Responsibilities

All Federal computer system users share certain general responsibilities for information resource protection. The following considerations should guide your actions.

- *Treat information as you would any valuable asset.*

You would not walk away from your desk leaving cash or other valuables unattended. You should take the same care to protect information. If you are not sure of the value or sensitivity of the various kinds of information you handle, ask your manager for guidance.

- *Use government computer systems only for lawful and authorized purposes.*

The computer systems you use in your daily work should be used only for authorized purposes and in a lawful manner. There are computer crime laws that prescribe criminal penalties for those who illegally access Federal computer systems or data. Additionally, the unauthorized use of Federal computer systems or use of authorized privileges for unauthorized purposes could result in disciplinary action.

- *Observe policies and procedures established by agency management.*

Specific requirements for the protection of information have been established by your agency. These requirements may be found in policy manuals, rules, or procedures. Ask your manager if you are unsure about your own responsibilities for protection of information.

- *Recognize that you are accountable for your activities on computer systems.*

After you receive authorization to use any Federal computer system, you become personally responsible and accountable for your activity on the system. Accordingly, your use should be restricted to those functions needed to carry out job responsibilities.

- *Report unusual occurrences to your manager.*

Many losses would be avoided if computer users would report any circumstances that seem unusual or irregular. Warning signals could include such things as unexplainable system activity that you did not perform, data that appears to be of questionable accuracy, and unexpected or incorrect processing results. If you should notice anything of a questionable nature, bring it to your manager's attention.

# Security and Control Guidelines

Some common-sense protective measures can reduce the risk of loss, damage, or disclosure of information. Following are the most important areas of information systems controls that assure that the system is properly used, resistant to disruptions, and reliable.

- *Make certain no one can impersonate you.*

If a password is used to verify your identity, this is the key to system security. Do not disclose your password to anyone, or allow anyone to observe your password as you enter it during the sign-on process. If you choose your own password, avoid selecting a password with any personal associations, or one that is very simple or short. The aim is to select a password that would be difficult to guess or derive. "1REDDOG" would be a better password than "DUKE."

If your system allows you to change your own password, do so regularly. Find out what your agency requires, and change passwords at least that frequently. Periodic password changes keep undetected intruders from continuously using the password of a legitimate user.

After you are logged on, the computer will attribute all activity to your user id. Therefore, never leave your terminal without logging off -- even for a few minutes. Always log off or otherwise inactivate your terminal so no one could perform any activity under your user id when you are away from the area.

- *Safeguard sensitive information from disclosure to others.*

People often forget to lock up sensitive reports and computer media containing sensitive data when they leave their work areas. Information carelessly left on top of desks and in unlocked storage can be casually observed, or deliberately stolen. Every employee who works with sensitive information should have lockable space available for storage when information is not in use. If you aren't sure what infor-

mation should be locked up or what locked storage is available, ask your manager.

While working, be aware of the visibility of data on your personal computer or terminal display screen. You may need to reposition equipment or furniture to eliminate over-the-shoulder viewing. Be especially careful near windows and in public areas. Label all sensitive diskettes and other computer media to alert other employees of the need to be especially careful. When no longer needed, sensitive information should be deleted or discarded in such a way that unauthorized individuals cannot recover the data. Printed reports should be finely shredded, while data on magnetic media should be overwritten. Files that are merely deleted are not really erased and can still be recovered.

- *Install physical security devices or software on personal computers.*

The value and popularity of personal computers make theft a big problem, especially in low-security office areas. Relatively inexpensive hardware devices greatly reduce the risk of equipment loss. Such devices involve lock-down cables or enclosures that attach equipment to furniture. Another approach is to place equipment in lockable cabinets.

When data is stored on a hard disk, take some steps to keep unauthorized individuals from accessing that data. A power lock device only allows key-holders to turn on power to the personal computer. Where there is a need to segregate information between multiple authorized users of a personal computer, additional security in the form of software is probably needed. Specific files could be encrypted to make them unintelligible to unauthorized staff, or access control software can divide storage space among authorized users, restricting each user to their own files.

- *Avoid costly disruptions caused by data or hardware loss.*

Disruptions and delays are expensive. No one enjoys working frantically to re-enter work, do the same job twice, or fix problems while new work piles up. Most disruptions can be prevented, and the impact of disruptions can be minimized by advance planning. Proper environmental conditions and power supplies minimize equipment out-

ages and information loss. Many electrical circuits in office areas do not constitute an adequate power source, so dedicated circuits for computer systems should be considered. Make certain that your surroundings meet the essential requirements for correct equipment operation. Cover equipment when not in use to protect it from dust, water leaks, and other hazards.

For protection from accidental or deliberate destruction of data, regular data backups are essential. Complete system backups should be taken at intervals determined by how quickly information changes or by the volume of transactions. Backups should be stored in another location, to guard against the possibility of original and backup copies being destroyed by the same fire or other disaster.

- *Maintain the authorized hardware/software configuration.*

Some organizations have been affected by computer "viruses" acquired through seemingly useful or innocent software obtained from public access bulletin boards or other sources; others have been liable for software illegally copied by employees. The installation of unauthorized hardware can cause damage, invalidate warranties, or have other negative consequences. Install only hardware or software that has been acquired through normal acquisition procedures and comply with all software licensing agreement requirements.

# SUMMARY

Ultimately, computer security is the user's responsibility. You, the user, must be alert to possible breaches in security and adhere to the security regulations that have been established within your agency. The security practices listed are not inclusive, but rather designed to remind you and raise your awareness towards securing your information resources:

**PROTECT YOUR EQUIPMENT**

- *Keep it in a secure environment*
- *Keep food, drink, and cigarettes* **AWAY** *from it*
- *Know where the fire suppression equipment is located and know how to use it*

**PROTECT YOUR AREA**

- *Keep unauthorized people AWAY from your equipment and data*
- *Challenge strangers in your area*

**PROTECT YOUR PASSWORD**

- *Never write it down or give it to anyone*
- *Don't use names, numbers or dates which are personally identified with you*
- *Change it often, but change it immediately if you think it has been compromised*

**PROTECT YOUR FILES**

- *Don't allow unauthorized access to your files and data*
- **NEVER** *leave your equipment unattended with your password activated* - **SIGN OFF!**

**PROTECT AGAINST VIRUSES**

- *Don't use unauthorized software*
- *Back up your files before implementing ANY new software*

**LOCK UP STORAGE MEDIA CONTAINING SENSITIVE DATA**

- *If the data or information is sensitive or critical to your operation, lock it up!*

**BACK UP YOUR DATA**

- *Keep duplicates of your sensitive data in a safe place, out of your immediate area*
- *Back it up as often as necessary*

**REPORT SECURITY VIOLATIONS**

- *Tell your manager if you see any unauthorized changes to your data*
- *Immediately report any loss of data or programs, whether automated or hard copy*

# For Additional Information

**National Institute of Standards and Technology**

Computer Security Program Office
A-216 Technology
Gaithersburg, MD 20899
(301) 975-5200

For further information on the management of information resources, NIST publishes Federal Information Processing Standards Publications (FIBS PUBS). These publications deal with many aspects of computer security, including password usage, data encryption, ADP risk management and contingency planning, and computer system security certification and accreditation. A list of current publications is available from:

Standards Processing Coordinator (ADP)
National Computer Systems Laboratory
National Institute of Standards and Technology
Technology Building, B-64
Gaithersburg, MD 20899
Phone: (301) 975-2817

NBS-114A (REV. 2-8C)

| U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET (See instructions) | 1. PUBLICATION OR REPORT NO. NIST/SP-500/171 | 2. Performing Organ. Report No. | 3. Publication Date October 1989 |
|---|---|---|---|

4. TITLE AND SUBTITLE

Computer User's Guide To The Protection Of Information Resources

5. AUTHOR(S)

Cheryl Helsing, Marianne Swanson, and Mary Anne Todd

6. PERFORMING ORGANIZATION (If joint or other than NBS, see instructions)

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
(formerly NATIONAL BUREAU OF STANDARDS)
U.S. DEPARTMENT OF COMMERCE
GAITHERSBURG, MD 20899

7. Contract/Grant No.

8. Type of Report & Period Covered

Final

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (Street, City, State, ZIP)

Same as item #6

10. SUPPLEMENTARY NOTES

Library of Congress Catalog Card Number: 89-600764

☐ Document describes a computer program; SF-185, FIPS Software Summary, is attached.

11. ABSTRACT (A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here)

Computers have changed the way we handle our information resources. Large amounts of information are stored in one central place with the ability to be accessed from remote locations. Users have a personal responsibility for the security of the system and the data stored in it. This document outlines the user's responsibilities and provides security and control guidelines to be implemented.

12. KEY WORDS (Six to twelve entries; alphabetical order; capitalize only proper names; and separate key words by semicolons)

controls; information resources; protective measures; risks; sensitive data; vulnerabilities

13. AVAILABILITY

☒ Unlimited

☐ For Official Distribution. Do Not Release to NTIS

☒ Order From Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.

☐ Order From National Technical Information Service (NTIS), Springfield, VA. 22161

14. NO. OF PRINTED PAGES 16

15. Price

## ANNOUNCEMENT OF NEW PUBLICATIONS ON COMPUTER SYSTEMS TECHNOLOGY

Superintendent of Documents
Government Printing Office
Washington, DC 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued in the series: National Institute of Standards and Technology Special Publication 500-.

Name _____

Company _____

Address _____

City _____ State _____ Zip Code _____

**(Notification key N-503)**

☆ U. S. Government Printing Office: 1989 - 251-395 (00899)

# NIST Technical Publications

## *Periodical*

**Journal of Research of the National Institute of Standards and Technology**—Reports NIST research and development in those disciplines of the physical and engineering sciences in which the Institute is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Institute's technical and scientific programs. Issued six times a year.

## *Nonperiodicals*

**Monographs**—Major contributions to the technical literature on various subjects related to the Institute's scientific and technical activities.

**Handbooks**—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

**Special Publications**—Include proceedings of conferences sponsored by NIST, NIST annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

**Applied Mathematics Series**—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

**National Standard Reference Data Series**—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NIST under the authority of the National Standard Data Act (Public Law 90-396). NOTE: The Journal of Physical and Chemical Reference Data (JPCRD) is published quarterly for NIST by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements are available from ACS, 1155 Sixteenth St., NW., Washington, DC 20056.

**Building Science Series**—Disseminates technical information developed at the Institute on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

**Technical Notes**—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NIST under the sponsorship of other government agencies.

**Voluntary Product Standards**—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NIST administers this program as a supplement to the activities of the private sector standardizing organizations.

**Consumer Information Series**—Practical information, based on NIST research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

*Order the* **above** *NIST publications from: Superintendent of Documents, Government Printing Office, Washington, DC 20402.*

*Order the* **following** *NIST publications—FIPS and NISTIRs—from the National Technical Information Service, Springfield, VA 22161.*

**Federal Information Processing Standards Publications (FIPS PUB)**—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NIST pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

**NIST Interagency Reports (NISTIR)**—A special series of interim or final reports on work performed by NIST for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Service, Springfield, VA 22161, in paper copy or microfiche form.

U.S. Department of Commerce
National Institute of Standards and Technology
(formerly National Bureau of Standards)
Gaithersburg, MD 20899