Management Guide to the Protection of Information Resources

National Institute of Standards and Technology
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 represents one activity towards the protection and management of sensitive information resources.

Acknowledgments

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

Executive Summary

Today computers are integral to all aspects of operations within an organization. As Federal agencies are becoming critically dependent upon computer information systems to carry out their missions, the agency executives (policy makers) are recognizing that computers and computer-related problems must be understood and managed, the same as any other resource. They are beginning to understand the importance of setting policies, goals, and standards for protection of data, information, and computer resources, and are committing resources for information security programs. They are also learning that primary responsibility for data security must rest with the managers of the functional areas supported by the data.

All managers who use any type of automated information resource system must become familiar with their agency's policies and procedures for protecting the information which is processed and stored within them. Adequately secure systems deter, prevent, or detect unauthorized disclosure, modification, or use of information. Agency information requires protection from intruders, as well as from employees with authorized computer access privileges who attempt to perform unauthorized actions. Protection is achieved not only by technical, physical and personnel safeguards, but also by clearly articulating and implementing agency policy regarding authorized system use to information users and processing personnel at all levels. This guide is one of three brochures that have been designed for a specific audience. The "Executive Guide to the Protection of Information Resources" and the "Computer User's Guide to the Protection of Information Resources" complete the series.

Table of Contents

Executive Summary iv
Introduction 1
Purpose of Guide 1
The Risks 1
Responsibilities 2
Information Systems Development 5
Control Decisions 5
Security Principles 5
Access Decisions 7
Systems Development Process 7
Computer Facility Management 9
Physical Security 9
Data Security 11
Monitoring and Review 11
Personnel Management 13
Personnel Security 13
Training 14
For Additional Information 15

Introduction

Purpose of this Guide

This guide introduces information systems security concerns and outlines the issues that must be addressed by all agency managers in meeting their responsibilities to protect information systems within their organizations. It describes essential components of an effective information resource protection process that applies to a stand alone personal computer or to a large data processing facility.

The Risks

Effort is required by every Federal agency to safeguard information resources and to reduce risks to a prudent level. The spread of computing power to individual employees via personal computers, local-area networks, and distributed processing has drastically changed the way we manage and control information resources. Internal controls and control points that were present in the past when we were dealing with manual or batch processes have not been established in many of today's automated systems. Reliance upon inadequately controlled computer systems can have serious consequences, including:

Inability or impairment of the agency's ability to perform its mission

Inability to provide needed services to the public

Waste, loss, misuse, or misappropriation of funds

Loss of credibility or embarrassment to an agency

To avoid these consequences, a broad set of information security issues must be effectively and comprehensively addressed.

Responsibilities

All functional managers have a responsibility to implement the policies and goals established by executive management for protection of automated information resources (data, processes, facilities, equipment, personnel, and information). Managers in all areas of an organization are clearly accountable for the protection of any of these resources assigned to them to enable them to perform their duties. They are responsible for developing, administering, monitoring, and enforcing internal controls, including security controls, within their assigned areas of authority. Each manager's specific responsibilities will vary, depending on the role that manager has with regard to computer systems.

Portions of this document provide more detailed information on the respective security responsibilities of managers of computer resources, managers responsible for information systems applications and the personnel security issues involved. However, all agency management must strive to:

Achieve Cost-Effective Security

The dollars spent for security measures to control or contain losses should never be more than the projected dollar loss if something adverse happened to the information resource.
Cost-effective security results when reduction in risk through implementation of safeguards is balanced with costs. The greater the value of information processed, or the more severe the consequences if something happens to it, the greater the need for control measures to protect it.
The person who can best determine the value or importance of data is the functional manager who is responsible for the data. For example, the manager responsible for the agency's budget program is the one who should establish requirements for the protection of the automated data which supports the program. This manager knows better than anyone else in the organization what the impact will be if the data is inaccurate or unavailable. Additionally, this manager usually is the supervisor of most of the users of the data.

It is important that these trade-offs of cost versus risk reduction be explicitly considered, and that management understand the degree of risk remaining after selected controls are implemented.

Assure Operational Continuity

With ever-increasing demands for timely information and greater volumes of information being processed, the threat of information system disruption is a very serious one. In some cases, interruptions of only a few hours are unacceptable. The impact due to inability to process data should be assessed, and actions should be taken to assure availability of those systems considered essential to agency operation. Functional management must identify critical computer applications and develop contingency plans so that the probability of loss of data processing and telecommunications support is minimized.

Maintain Integrity

Integrity of information means you can trust the data and the processes that manipulate it. Not only does this mean that errors and omissions are minimized, but also that the information system is protected from deliberate actions to wrongfully change the data. Information can be said to have integrity when it corresponds to the expectations and assumptions of the users.

Assure Confidentiality

Confidentiality of sensitive data is often, but not always, a requirement of agency systems. Privacy requirements for personal information is dictated by statute, while confidentiality of other agency information is determined by the nature of that information, e.g., information submitted by bidders in procurement actions. The impact of wrongful disclosure must be considered in understanding confidentiality requirements.

Comply with Applicable Laws and Regulations

As risks and vulnerabilities associated with information systems become better understood, the body of law and regulations compelling positive action to protect information resources grows. OMB Circular No. A-130, "Management of Federal Information Resources" and Public Law 100-235, "Computer Security Act of 1987" are two documents where the knowledge of these regulations and laws provide a baseline for an information resource security program.

Information Systems Development

This section describes the protective measures that should be included as part of the design and development of information processing application systems. The functional manager that is responsible for and will use the information contained in the system, must ensure that security measures have been included and are adequate. This includes applications designed for personal computers as well as large mainframes.

Control Decisions

The official responsible for the agency function served by the automated information system has a critical role in making decisions regarding security and control. In the past, risk was often unconsciously accepted when such individuals assumed the computer facility operators were taking care of security. In fact, there are decisions to be made and security elements to be provided that cannot be delegated to the operator of the system. In many cases, the user or manager develops the application and operates solely.

The cost of control must be balanced with system efficiency and usability issues. Risk must be evaluated and cost-effective controls selected to provide a prudent level of control while maximizing productivity. Controls are often closely connected with the system function, and cannot be effectively designed without significant understanding of the process being automated.

Security Principles

There are some common security attributes that should be present in any system that processes valuable personal or sensitive information. System designs should include mechanisms to enforce the following security attributes.

Identification and Authentication of Users

Each user of a computer system should have a unique identification on the system, such as an account number or other user identification code. There must also be a means of verifying that the individual claiming that identity (e.g., by typing in that identifying code at a terminal) is really the authorized individual and not an imposter. The most common means of authentication is by a secret password, known only to the authorized user.

Authorization Capability Enforcing the Principle of Least Possible Privilege

Beyond ensuring that only authorized individuals can access the system, it is also necessary to limit the users access to information and transaction capabilities. Each person should be limited to only the information and transaction authority that is required by their job responsibilities. This concept, known as the principle of least possible privilege, is a long-standing control practice. There should be a way to easily assign each user just the specific access authorities needed.

Individual Accountability

From both a control and legal point of view, it is necessary to maintain records of the activities performed by each computer user. The requirements for automated audit trails should be developed when a system is designed. The information to be recorded depends on what is significant about each particular system. To be able to hold individuals accountable for their actions, there must be a positive means of uniquely identifying each computer user and a routinely maintained record of each user's activities.

Audit Mechanisms

Audit mechanisms detect unusual events and bring them to the attention of management. This commonly occurs by violation reporting or by an immediate warning to the computer system operator. The type of alarm generated depends on the seriousness of the event.

A common technique to detect access attempts by unauthorized individuals is to count attempts. The security monitoring functions of the system can automatically keep track of unsuccessful attempts to gain access and generate an alarm if the attempts reach an unacceptable number.

Performance Assurance

A basic design consideration for any information system should be the ability to verify that the system is functioning as intended. Systems that are developed without such design considerations are often very difficult to independently audit or review, leading to the possibility of unintended results or inaccurate processing.

Recoverability

Because Federal agencies can potentially be heavily dependent on a computer system, an important design consideration is the ability to easily recover from troublesome events, whether minor problems or major disruptions of the system. From a design point of view, systems should be designed to easily recover from minor problems, and to be either transportable to another backup computer system or replaced by manual processes in case of major disruption or loss of computer facility.

Access Decisions

Once the automated system is ready to use, decisions must be made regarding access to the system and the information it contains. For example, many individuals require the ability to access and view data, but not the ability to change or delete data. Even when computer systems have been designed to provide the ability to narrowly designate access authorities, a knowledgeable and responsible official must actually make those access decisions. The care that is taken in this process is a major determining factor of the level of security and control present in the system. If sensitive data is being transmitted over unprotected lines, it can be intercepted or passive eavesdropping can occur. Encrypting the files will make the data unintelligible and port protection devices will protect the files from unauthorized access, if warranted.

Systems Development Process

All information systems software should be developed in a controlled and systematic manner according to agency standards. The quality and efficiency of the data processed, and the possible reconfiguration of the system can all be affected by an inadequate development process. The risk of security exposures and vulnerabilities is greatly reduced when the systems development process is itself controlled.

Computer Facility Management

Functional managers play a critical role in assuring that agency information resources are appropriately safeguarded. This section describes the protective measures that should be incorporated into the ongoing management of information resource processing facilities. As defined in OMB Circular No. A-130, "Management of Federal Information Resources," the term "information technology facility" means an organizationally defined set of personnel, hardware, software, and physical facilities, a primary function of which is the operation of information technology. This section, therefore applies to any manager who houses a personal computer, mainframe or any other form of office system or automated equipment.

Physical Security

Information cannot be appropriately protected unless the facilities that house the equipment are properly protected from physical threats and hazards. The major areas of concern are described below.

Environmental Conditions

For many types of computer equipment, strict environmental conditions must be maintained. Manufacturer's specifications should be observed for temperature, humidity, and electrical power requirements.

Control of Media

The media upon which information is stored should be carefully controlled. Transportable media such as tapes and cartridges should be kept in secure locations, and accurate records kept of the location and disposition of each. In addition, media from an external source should be subject to a check-in process to ensure it is from an authorized source.

Control of Physical Hazards

Each area should be surveyed for potential physical hazards. Fire and water are two of the most damaging forces with regard to computer systems. Opportunities for loss should be minimized by an effective fire detection and suppression mechanism, and planning reduces the danger of leaks or flooding. Other physical controls include reducing the visibility of the equipment and strictly limiting access to the area or equipment.

Contingency Planning

Although risks can be minimized, they cannot be eliminated. When reliance upon a computer facility or application is substantial, some type of contingency plan should be devised to allow critical systems to be recovered following a major disaster, such as a fire. There are a number of alternative approaches that should be evaluated to most cost-effectively meet the agency's need for continuity of service.

Configuration Management

Risk can be introduced through unofficial and unauthorized hardware or software. Another key component of information resource management is ensuring only authorized hardware and software are being utilized. There are several control issues to be addressed.

Maintaining Accurate Records

Records of hardware/software inventories, configurations, and locations should be maintained and kept up-to-date.

Complying with Terms of Software Licenses

Especially with microcomputer software, illegal copying and other uses in conflict with licensing agreements are concerns.

The use of software subject to licensing agreements must be monitored to ensure it is used according to the terms of the agreement.

Protecting Against Malicious Software and Hardware

The recent occurrences of destructive computer "viruses" point to the need to ensure that agencies do not allow unauthorized software to be introduced to their computer environments. Unauthorized hardware can also contain hidden vulnerabilities. Management should adopt a strong policy against unauthorized hardware/software, inform personnel about the risks and consequences of unauthorized additions to computer systems, and develop a monitoring process to detect violations of the policy.

Data Security

Management must ensure that appropriate security mechanisms are in place that allow responsible officials to designate access to data according to individual computer users' specific needs. Security mechanisms should be sufficient to implement individual authentication of system users, allow authorization to specific information and transaction authorities, maintain audit trails as specified by the responsible official, and encrypt sensitive files if required by user management.

Monitoring and Review

A final aspect of information resource protection to be considered is the need for ongoing management monitoring and review. To be effective, a security program must be a continuous effort. Ideally, ongoing processes should be adapted to include information protection checkpoints and reviews. Information resource protection should be a key consideration in all major computer system initiatives.

Earlier, the need for system audit trails was discussed. Those audit trails are useful only if management regularly reviews exception items or unusual activities. Irregularities should be researched and action taken when merited. Similarly, all information-related losses and incidents should be investigated.

A positive benefit of an effective monitoring process is an increased understanding of the degree of information-related risk in agency operations. Without an ongoing feedback process, management may unknowingly accept too much risk. Prudent decisions about trade-offs between efficiency and control can only be made with a clear understanding of the degree of inherent risk. Every manager should ask questions and periodically review operations to judge whether changes in the environment have introduced new risk, and to ensure that controls are working effectively.

Personnel Management

Managers must be aware that information security is more a people issue than a technical issue. Personnel are a vital link in the protection of information resources, as information is gathered by people, entered into information resource systems by people, and ultimately used by people. Security issues should be addressed with regard to:

People who use computer systems and store information in the course of their normal job responsibilities

People who design, program, test, and implement critical or sensitive systems

People who operate computer facilities that process critical or sensitive data

Personnel Security

From the point of hire, individuals who will have routine access to sensitive information resources should be subject to special security procedures. More extensive background or reference checks may be appropriate for such positions, and security responsibilities should be explicitly covered in employee orientations. Position descriptions and performance evaluations should also explicitly reference unusual responsibilities affecting the security of information resources.

Individuals in sensitive positions should be subject to job rotation, and work flow should be designed in such a way as to provide as much separation of sensitive functions as possible. Upon decision to terminate or notice of resignation, expedited termination or rotation to less sensitive duties for the remainder of employment is a reasonable precaution.

Any Federal computer user who deliberately performs or attempts to perform unauthorized activity should be subject to disciplinary action, and such disciplinary action must be uniformly applied throughout the agency. Any criminal activity under Federal or state computer crime laws must be reported to law enforcement authorities.

Training

Most information resource security problems involve people. Problems can usually be identified in their earliest stages by people who are attuned to the importance of information protection issues. A strong training program will yield large benefits in prevention and early detection of problems and losses. To be most effective, training should be tailored to the particular audience being addressed, e.g., executives and policy makers; program and functional managers; IRM security and audit: ADP management and operations; end users.

Most employees want to do the right thing, if agency expectations are clearly communicated. Internal policies can be enforced only if staff have been made aware of their individual responsibilities. All personnel who access agency computer systems should be aware of their responsibilities under agency policy, as well as obligations under the law. Disciplinary actions and legal penalties should be communicated.

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