

EXECGUIDE.TXT

Executive 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 telecommunications 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 "Managers Guide to the Protection of Information Resources" and the "Computer User's 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, National Institute of Standards and Technology.

Table of Contents

Introduction	1
Executive Responsibilities	3
Executive Goals	5
Information Protection Program Elements	7
Information Protection Program Implementation	11
For Additional Information	15
Introduction	

Federal agencies are becoming increasingly dependent upon automated information systems to carry out their missions. While in the past, executives have taken a hands-off approach in dealing with these resources, essentially leaving the area to the computer technologist, they are now recognizing that computers and computer-related problems must be understood and managed, the same as any other resource.

The success of an information resources protection program depends on the policy generated, and on the attitude of management toward securing information on automated systems. You, the policy maker, set the tone and the emphasis on how important a role information security will have within your agency. Your primary responsibility is to set the information

EXEGUIDE.TXT

resource security policy for the organization with the objectives of reduced risk, compliance with laws and regulations and assurance of operational continuity, information integrity, and confidentiality.

Purpose of this Guide

This guide is designed to help you, the policy maker, address a host of questions regarding the protection and safety of computer systems and data processed within your agency. It introduces information systems security concerns, outlines the management issues that must be addressed by agency policies and programs, and describes essential components of an effective implementation process.

The Risks

The proliferation of 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 always been replaced with comparable controls in many of today's automated systems. Reliance upon inadequately controlled information 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 addressed effectively and comprehensively. Towards this end, executives should take a traditional risk management approach, recognizing that risks are taken in the day-to-day management of an organization, and that there are alternatives to consider in managing these risks. Risk is accepted as part of doing business or is reduced or eliminated by modifying operations or by employing control mechanisms.

Executive Responsibilities

Set the Security Policy of the Organization

Protecting information resources is an important goal for all organizations. This goal is met by establishing an information resource security program. It will require staff, funding and positive incentives to motivate employees to

EXEGUIDE.TXT

participate in a program to protect these valuable assets.
This information resource protection policy should
state precisely:

the value to the agency of data and information
resources and the need to preserve their integrity, availability,
and confidentiality

the intent of the organization to protect the resources
from accidental or deliberate unauthorized disclosure,
modification, or destruction by employing cost-effective controls

the assignment of responsibility for data security
throughout the organization

the requirement to provide computer security and
awareness training to all employees having access to information
resources

the intent to hold employees personally accountable for
information resources entrusted to them

the requirement to monitor and assess data security via
internal and external audit procedures

the penalties for not adhering to the policy

Executive Goals

The policy established for securing information
resources should meet the basic goals of reducing the risk,
complying with applicable laws and regulations, and assuring
operational continuity, integrity and confidentiality. This
section briefly describes these objectives and how they can be
met.

Reduce Risk To An Acceptable Level

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

EXEGUIDE.TXT

Assure Operational Continuity

With ever-increasing demands for timely information and greater volumes of information being processed, availability of essential systems, networks, and data is a major protection issue. In some cases, service disruptions of just a few hours are unacceptable. Agency reliance on essential computer systems requires that advance planning be done to allow timely restoration of processing capabilities in the event of severe service disruption. The impact due to inability to process data should be assessed, and action taken to assure availability of those systems considered essential to agency operation.

Comply with Applicable Laws and Regulations

As the pervasiveness of computer systems increases and the 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 systems," and Public Law 100-235, "Computer Security Act of 1987" are two documents where the knowledge of these laws provide a baseline for an information resources security program.

Assure Integrity and Confidentiality

An important objective of an information resource management program is to ensure that the information is accurate. Integrity of information means you can trust the data and the processes that manipulate it. A system has integrity when it provides sufficient accuracy and completeness to meet the needs of the user(s). It should be properly designed to automate all functional requirements, include appropriate accounting and integrity controls, and accommodate the full range of potential conditions that might be encountered in its operation.

Agency information should also be protected from intruders, as well as from employees with authorized computer access privileges who attempt to perform unauthorized actions. Assured confidentiality of sensitive data is often, but not always, a requirement of agency systems. Privacy requirements for personal information are generally dictated by statute, while protection requirements for other agency information are a function of the nature of that information. Determination of requirements in the latter case is made by the official responsible for that information. The impact of wrongful disclosure should be considered in understanding confidentiality requirements.

Information Protection Program Elements

EXEGUIDE.TXT

Need for Policies and Procedures

Successful execution of the responsibilities previously outlined requires establishing agency policies and practices regarding information protection. The security policy directive facilitates consistent protection of information resources. Supporting procedures are most effectively implemented with top management support, through a program focused on areas of highest risk. A compliance assessment process ensures ongoing effectiveness of the information protection program throughout the agency.

Scope

Although the protection of automated information resources is emphasized in this publication, protection requirements will usually extend to information on all forms of media. Agency programs should apply safeguards to all information requiring protection, regardless of its form or location. Comprehensive information resource protection procedures will address: accountability for information, vulnerability assessment, data access, hardware/software control, systems development, and operational controls. Protection should be afforded throughout the life cycle of information, from creation through ultimate disposition.

Accountability for Information

An effective information resource protection program identifies the information used by the agency and assigns primary responsibility for information protection to the managers of the respective functional areas supported by the data. These managers know the importance of the data to the organization and are able to quantify the economic consequences of undesirable happenings. They are also able to detect deficiencies in data and know definitively who must have access to the data supporting their operations. A fundamental information protection issue is assignment of accountability. Information flows throughout the organization and can be shared by many individuals. This tends to blur accountability and disperse decision-making regarding information protection. Accountability should be explicitly assigned for determining and monitoring security for appropriate agency information.

When security violations occur, management must be accountable for responding and investigating. Security violations should trigger a re-evaluation of access authorizations, protection decisions, and control techniques. All apparent violations should be resolved; since absolute protection will never be achieved, some losses are inevitable. It is important, however, that the degree of risk assumed be

EXEGUIDE.TXT

commensurate with the sensitivity or importance of the information resource to be protected.

Vulnerability Assessment

A risk assessment program ensures management that periodic reviews of information resources have considered the degree of vulnerability to threats causing destruction, modification, disclosure, and delay of information availability, in making protection decisions and investments in safeguards. The official responsible for a specific information resource determines protection requirements. Less-sensitive, less-essential information will require minimal safeguards, while highly sensitive or critical information might merit strict protective measures. Assessment of vulnerability is essential in specifying cost-effective safeguards; overprotection can be needlessly costly and add unacceptable operational overhead.

Once cost-effective safeguards are selected, residual risk remains and is accepted by management. Risk status should be periodically re-examined to identify new threats, vulnerabilities, or other changes that affect the degree of risk that management has previously accepted.

Data Access

Access to information should be delegated according to the principles of need-to-know and least possible privilege. For a multi-user application system, only individuals with authorized need to view or use data are granted access authority, and they are allowed only the minimum privileges needed to carry out their duties. For personal computers with one operator, data should be protected from unauthorized viewing or use. It is the individual's responsibility to ensure that the data is secure.

Systems Development

All information systems software should be developed in a controlled and systematic manner according to agency standards. Agency policy should require that appropriate controls for accuracy, security, and availability are identified during system design, approved by the responsible official, and implemented. Users who design their own systems, whether on a personal computer or on a mainframe, must adhere to the systems development requirements.

Systems should be thoroughly tested according to accepted standards and moved into a secure production environment through a controlled process. Adequate documentation should be

EXEGUIDE.TXT

considered an integral part of the information system and be completed before the system can be considered ready for use.

Hardware/Software Configuration Control

Protection of hardware and resources of computer systems and networks greatly contributes to the overall level of control and protection of information. The information protection policies should provide substantial direction concerning the management and control of computer hardware and software.

Agency information should be protected from the potentially destructive impact of unauthorized hardware and software. For example, software "viruses" have been inserted into computers through games and apparently useful software acquired via public access bulletin boards; viruses can spread from system to system before being detected. Also, unauthorized hardware additions to personal computers can introduce unknown dial-in access paths. Accurate records of hardware/software inventory, configurations, and locations should be maintained, and control mechanisms should provide assurance that unauthorized changes have not occurred.

To avoid legal liability, no unauthorized copying of software should be permitted. Agencies should also address the issue of personal use of Federal computer systems, giving employees specific direction about allowable use and providing consistent enforcement.

Operational Controls

Agency standards should clearly communicate minimum expected controls to be present in all computer facilities, computer operations, input/output handling, network management, technical support, and user liaison. More stringent controls would apply to those areas that process very sensitive or critical information.

Protection of these areas would include:

- Security management;
- Physical security;
- Security of system/application software and data;
- Network security; and
- Contingency planning.

The final section of this guide describes the organizational process of developing, implementing, and managing the ongoing information protection program.

Information Protection Program Implementation

Information Protection Management

In most cases, agency executive management is not directly involved in the details of achieving a controlled information processing environment. Instead, executive action should focus on effective planning, implementation, and an ongoing review structure. Usually, an explicit group or organization is assigned specific responsibility for providing day-to-day guidance and direction of this process. Within this group an information security manager (ISM) should be identified as a permanent focal point for information protection issues within the agency.

The ISM must be thoroughly familiar with the agency mission, organization, and operation. The manager should have sufficient authority to influence the organization and have access to agency executives when issues require escalation.

Independence

In determining the reporting relationship of the ISM, independence of functional areas within the agency is desirable. Plans and budget for the ISM function should be approved by agency management, rather than being part of any functional area budget. This approach avoids conflicts of interest and facilitates development and maintenance of a comprehensive and consistent protection program that serves the needs of agency management.

Degree of Centralization

The desirability of centralized versus decentralized security is heavily debated and largely depends on size, organizational structure, and management approach at the individual agency. A centralized approach to security has the advantages of being directly responsive to executive direction and specifically accountable for progress and status.

A decentralized approach to security has the advantages of being close to the functional area involved. In the long term, decentralization may provide better integration of security with other entity functions.

An effective combined approach offers advantages.

A small dedicated resource at the agency level can direct the information protection program, while additional resources are utilized at the functional area level to implement the program in each area.

Dedicated Staff

EXEGUIDE.TXT

The common practice of assigning responsibility for information security to existing staff with other major responsibilities is often unsuccessful. At least one dedicated staff member is recommended at the program management level. The need for additional full-time resources depends on the agency's computer environment. The number of information systems, their technical complexity, the degree of networking, the importance of information processed, adequacy of existing controls, and extent of agency dependence on information systems affect the resources needed.

Implementation Stages

Development of a comprehensive information protection program that is practiced and observed widely throughout a Federal agency occurs in stages and requires ongoing monitoring and maintenance to remain viable.

First, organizational requirements for information protection are identified. Different agencies have varying levels of need for security, and the information protection program should be structured to most effectively meet those needs.

Next, organizational policies are developed that provide a security architecture for agency operations, taking into consideration the information protection program elements discussed in the previous section of this guide. The policies undergo normal review procedures, then are approved by agency management for implementation.

Activities are then initiated to bring the agency into compliance with the policies. Depending on the degree of centralization, this might require development of further plans and budgets within functional entities of the agency to implement the necessary logical and physical controls.

Training

Training is a major activity in the implementation process. Security violations are the result of human action, and problems can usually be identified in their earliest stages by people. Developing and maintaining personnel awareness of information security issues can yield large benefits in prevention and early detection of problems and losses.

Target audiences for this training are executives and policy makers, program and functional managers, IRM security and audit personnel, computer management and operations, and end users. Training can be delivered through existing policy and

EXEGUIDE.TXT

procedures manuals, written materials, presentations and classes, and audio-visual training programs.

The training provided should create an awareness of risks and the importance of safeguards, underscoring the specific responsibilities of each of the individuals being trained.

Monitoring and Enforcement

An ongoing monitoring and enforcement program assures continued effectiveness of information protection measures. Compliance may be measured in a number of ways, including audits, management reviews or self-assessments, surveys, and other informal indicators. A combination of monitoring mechanisms provides greater reliability of results.

Variances from policy requirements should be accepted only in cases where the responsible official has evaluated, documented, and accepted the risk of noncompliance. Enforcement of agency policies and practices is important to the overall success of an information protection program. Inconsistent or lax enforcement quickly results in deterioration of internal controls over information resources.

A positive benefit of an effective monitoring and enforcement process is an increased understanding of the degree of information-related risk in agency operations. Without such a feedback process, management unknowingly accepts too much risk. An effective information protection program allows the agency to continue to rely upon and expand the use of information technology while maintaining an acceptable level of risk.

Maintenance

As agency initiatives and operations change, and as the computer environment evolves, some elements of the information protection program will require change as well. Information protection cannot be viewed as a project with a distinct end; rather, it is a process that should be maintained to be realistic and useful to the agency. Procedures for review and update of policies and other program elements should be developed and followed.

For Additional Information

National Institute Of Standards and Technology
Computer Security Program Office
A-216 Technology
Gaithersburg, MD 20899

EXEGUIDE.TXT

(301) 975-5200

For further information on the management of information resources, NIST publishes Federal Information Processing Standards Publications (FIPS 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

Downloaded From P-80 International Information Systems 304-744-2253