THE CITY OF NEW YORK
OFFICE OF THE COMPTROLLER

INTERNAL CONTROL AND ACCOUNTABILITY DIRECTIVE

DIRECTIVE 18 - GUIDELINES FOR THE MANAGEMENT, PROTECTION AND CONTROL OF AGENCY INFORMATION AND INFORMATION PROCESSING SYSTEMS

INTRODUCTION AND SUMMARY

This Directive provides Agency Heads with a guide to the management, protection and control of automated information systems, data processing resources and the data and information stored in automated systems. It identifies primary areas of management concern, risks common to information processing environments, and provides an overview of basic tools and techniques available to assist Agency Heads in the management and control of this critical area.

The protection and control of data and information processing resources is an important element of the agency's overall internal control environment. As with the protection of any other asset, the primary responsibility for safeguarding the agency's data and information processing resources resides with Agency Heads and agency executive management. Agency Heads can insure that adequate internal controls over these assets have been established by insisting on compliance with the control practices and procedures provided in this Directive.

Compliance with this Directive will help agency managers conform with Section 389 of the New York City Charter which requires Agency Heads to maintain an internal control environment that maximizes the effectiveness and integrity of agency operations and reduces the agency's vulnerability to fraud, waste, abuse, error, conflict of interest, and corruption. The Directive provides the foundation policies, procedures and methods that are necessary to create and maintain a control environment tailored to specific agency information protection needs, and that will help insure the effective management of this aspect of agency operations.

1.0 GENERAL INFORMATION

1.1 Directive Organization

1.0 General Information

PART I: CONCEPTS, MANAGEMENT & PLANNING

2.0 Underlying Concepts and Discussion
3.0 Abstract of Executive Management's Role
4.0 Assessing the Internal Control Environment
5.0 The Information Protection Plan

PART II: INTERNAL CONTROLS FOR INFORMATION PROCESSING ENVIRONMENTS

6.0 Organizational and Personnel Controls
7.0 The Physical Environment
8.0 Software Based Controls
9.0 Operational and General Controls
10.0 Business Continuation (Disaster Recovery) Plans

PART III: MONITORING PERFORMANCE AND RESULTS

11.0 Monitoring Performance and Results

APPENDIX A: Additional Sources and Information
APPENDIX B: Federal Government Agency Publications

1.2 Effective Date

This Directive is effective immediately. The August 1981 version entitled, *Guidelines for Computer Security and Control* is superseded.

1.3 Directive Scope and Content

Agencies should view this Directive as an outline of the general controls, practices and procedures that are necessary to adequately protect data processing resources. It is not a ready-made policy for any agency's particular situation. Agencies are encouraged to supplement the Directive with the wealth of management, operational and technical publications that are available from Federal and other sources. The Directive's text, and a more comprehensive listing in Appendices A and B provide references to the National Institute of Standards and Technology's (NIST) publications which are widely accepted as authoritative guidelines for use in the management, control and design of information processing resources. Appendix B provides additional detail on how specific NIST documents can be obtained.

PART I: CONCEPTS, MANAGEMENT & PLANNING

2.0 UNDERLYING CONCEPTS AND DISCUSSION

This section introduces the broad issues facing agencies that rely on computers and data processing, and sets forth a general approach to the management, protection and control of data and information processing resources.

2.1 The Dynamic Nature of Information Processing

Data processing has undergone a series of major transformations since the prior version of this Directive was issued in 1981. At the time, the typical information processing environment consisted primarily of a relatively easy to secure, centrally located computer with a rigidly defined network of terminals that had limited capabilities. Risks were relatively easy to identify and contain.

Existing environments are very different. Critical data and information can now reside in a variety of locations ranging from large centralized computers, to networked servers, to versatile desktop computers. There have been quantum increases in the power of desktop computers and the capacity of physically dispersed storage devices. The number and variety of access paths into and out of computer networks have multiplied dramatically, i.e., information can easily be transmitted over agency networks, citywide networks, or through the publically accessible Internet. Software and data files are highly portable and interchangeable. All of these factors have vastly increased agency risk exposure.

Agencies are faced with the further challenge of managing in an environment where information technology continues to change rapidly. New products with new capabilities, often representing not only greater functionality, but also, potentially greater risks, continually enter the marketplace.

2.2 The Information Processing Environment Defined

All of the elements of an agency's information processing systems, including the hardware, the software, the telecommunications, the networks, and the data and information resident in the agency's computers and computer systems collectively make up its "information processing environment". This term is used throughout this Directive as a combined reference to the tangible elements as well as the software and the data.

Information processing environments vary widely from agency to agency. They can range from large, complex systems running on an extensive network, to stand alone desktop workstations. There are literally thousands of products available for agency use and countless ways that these products can be combined to serve agency information processing needs. In the City of New York, service providers such as the Financial Information Services Agency (FISA) and the Department of Information and Telecommunications Technology (DoITT) constitute part of the information processing environment mix for most agencies.

2.3 Focus on Information

Both the physical components of the information processing environment and the electronic data and information it contains are susceptible to damage, destruction, theft and inappropriate use.

Computer stored information is an asset, in many respects, no different than the computer hardware itself and the other more traditional assets under agency control. By focusing on the information, management will recognize that the physical system is not an end unto itself, but exists because of the information it contains, and that the information stored in agency systems has been collected at a significant cost that can far exceed the cost of the system's physical components.

As with more tangible assets, electronic information is subject to a number of hazards. It too, can be stolen, tampered with and misappropriated, but it can also be made useless by the introduction of unintentional or purposeful errors, lost, diverted to unauthorized individuals for profit or other uses, and viewed without authorization by casual browsers. Additional exposure exists with respect to information because its disclosure can be restricted by statutory or other confidentiality requirements resulting in potential liability to the City. Another risk of corrupted information is the potential adverse impact that erroneous information can have on the agency's general business or strategic decisions. Because information, for the most part, is intangible, its protection requires a specialized set of rules and procedures.

3.0 ABSTRACT OF EXECUTIVE MANAGEMENT'S ROLE

This section introduces the principal aspects of the Agency Head's and executive management's responsibilities for managing the information processing environment and for implementing effective internal controls, policies, and procedures. Each area of responsibility is referenced, where applicable, to subsequent sections in the Directive where greater detail is provided. The size and complexity of the information processing environment and the degree to which an agency relies upon it impact the level of effort Agency Heads will need to devote to adequately manage this aspect of agency operations.

3.1 Setting the Tone

Protecting the information processing environment is a specialized area of the overall internal control environment described in Comptroller's Internal Control and Accountability Directive #1, *City Manager Financial Integrity Statement*. The policies and procedures set forth in this Directive are consistent with the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) model published in its 1992 report, *Internal Control - Integrated Framework.* As in other aspects of agency operations, the Agency Head is ultimately responsible for protecting the information processing environment and has the obligation of setting the "tone at the top" to promote agency wide focus on the protection of information systems, data and resources.

A critical Agency Head role is to recognize the importance of information processing environment protection and provide leadership and direction to the executive managers and the senior managers who have primary responsibility for business operations and for the operation of the agency's computer systems. The Agency Head can execute this duty by establishing an information protection program which ensures that security exposures are assessed, that appropriate organizational policies, practices and procedures are established, that the policies and procedures described in the agency's information protection plan are communicated to all appropriate staff, and that there is agency wide compliance.

3.2 Internal Control Environment Assessment

A practical way for the Agency Head to approach the management and control of the agency's information processing environment is to conduct a comprehensive assessment of the agency's data processing policies, practices and internal controls. The assessment involves inventorying the agency's information, data, data processing equipment and systems, and making objective assessments of the risks associated with those assets, of the controls and the protective measures in place, and of the agency's vulnerabilities. To achieve the maximum benefit from the assessment, it is important for the Agency Head to insure that it is conducted at an appropriately responsible level in the organization. More detailed guidance for conducting the assessment is provided in §4.0, *Assessing the Internal Control Environment.*

3.3 Developing the Information Protection Plan

After conducting the internal control assessment, the Agency Head is responsible for insuring that the risks and vulnerabilities disclosed in the assessment are adequately addressed by requiring the development of a formal information processing environment protection plan. Section 5.0, *The Information Protection Plan,* describes the key elements of information protection plans and can serve as an outline or starting point for the agency's program.

Part II of this Directive, *Internal Controls for Information Processing Environments,* contains more specific guidance on the internal controls, procedures, and other activities that can be used to manage and protect the information processing environment. Incorporating the controls, policies and procedures provided in Part II into the agency's information protection plan, as appropriate, will help insure the plan's effectiveness.

3.4 Creating the Appropriate Organizational Structure

It is vital that Agency Heads adequately staff information processing environment functions with personnel who have the appropriate training and experience, and adequately segregate job functions to insure that conflicting responsibilities are independently managed. Proper segregation of duties helps prevent fraudulent acts and maximizes the potential for detection of unauthorized, illegal or other inappropriate acts or events. Organizational, personnel and segregation of duties requirements are discussed in greater detail in §6.0, *Organizational and Personnel Controls*.

3.5 Information Protection Plan Updates

After the information protection plan is initially implemented, periodic reviews and/or updates at least once every two years, preferably more frequently, will insure that it continues to appropriately protect against risks. An important Agency Head role is to insure that the assessment of the information processing environment and the maintenance of the protection plan is a continuous, ongoing process. Regular updating is especially important because of the rapidity of technology changes, the continuous development of new applications, and the trend toward maintaining more and different data on information systems. The review must also consider changes in threats and vulnerabilities, business operations, and the organizational structure. Previously unaddressed problems highlighted by ongoing performance monitoring and internal audits should be addressed when modifying the plan.

3.6 Business Continuation Preparedness and Planning

An important Agency Head responsibility is to recognize the degree to which a sudden and sustained major loss or disruption of computer processing capability would impact the agency's ability to provide its services or fulfill its mission. The effort and resources devoted to preparing for such events is dependent on the agency's willingness to bear the risk of not being able to provide services or conduct critical agency business. Factors which must be considered include the likelihood of such events occurring, the severity and length of the loss or disruption, and the cost of the contingency plan. Agency Heads can insure that the business recovery plan is kept current by requiring that it be tested periodically. Business continuation planning is discussed in §10.0, *Business Continuation (Disaster Recovery) Plans*.

3.7 Monitoring Information Processing Environment Performance

A key Agency Head role is to insure that timely, accurate and focused feedback describing the performance of the agency's systems and the workings of the information processing environment and its internal controls are routinely brought to executive management's attention for review and action if necessary. Agency Heads can obtain this information in a number of ways including exception and violation reporting, service performance reporting, end user satisfaction reports, quality assurance programs, and internal audits. Techniques for monitoring performance and results are discussed in greater detail in Part III: *Monitoring Performance and Results.*

3.8 Additional Information

Additional guidance geared to executive and senior managers include NIST Publication SP 500-169, *Executive Guide to the Protection of Information Resources*, and SP 500-170, *Management Guide to the Protection of Information Resources.*

4.0 ASSESSING THE INTERNAL CONTROL ENVIRONMENT

Performing a careful and comprehensive assessment of the agency's internal control environment for information processing is a crucial first step in the protection and control of agency information processing environments. The assessment process includes collecting the fundamental information and doing the analyses necessary to create an effective information protection plan.

The assessment and analyses will help the agency make informed decisions about the amount of effort and resources to be incorporated into the information protection plan and will help agencies direct their resources to the most important agency information and information processing system components. Independent or internal audit staff should be engaged in the assessment process.

For agencies that already have an information protection plan or elements of a plan in place, the assessment will help evaluate its strengths and weaknesses.

4.1 Information Processing Environment Inventory

The first step in evaluating the information processing environment is to conduct an inventory of the agency's data and information and its collection, processing, storage and delivery systems and equipment. Conducting the inventory involves:

(1) Identifying every agency business function that relies on information processing systems.

(2) Identifying the automated systems and software products that support each business function, including the numbers and types of software licenses owned and in use.

(3) Identifying the data and information that is processed in each system or software product.

(4) Locating and recording the physical components of the data processing environment including, but not limited to, networks, telecommunication lines, computers, servers, printers, switching devices, and environmental control equipment such as air conditioners and power conditioners.

4.2 Categorizing the Importance of Information and Other Information Processing Assets

This step assesses the impact that a loss in the integrity, confidentiality, or availability of the data in each computer or computer system would have to the agency. In conducting this analysis agencies must recognize that all information is not equally important.

4.2.1 Categorize Information Impact

One measure of importance is the impact that the loss of data would have on the agency's ability to fulfill its mission. Information may be highly critical to the agency's mission, important, but not critical to the mission, or of minor or lesser significance to the agency's mission. Agencies should develop categories most appropriate to their business. An important consideration in rating impact on business operations is the maximum time the agency can function without the information.

4.2.2 Categorize Information Confidentiality

Another measure of data importance is its confidentiality level. Typical categories include highly confidential, need to know, and publicly available. The agency's legal obligation to keep certain data confidential must be considered. Again, agencies should create categories that are most meaningful to their own situations.

4.2.3 Categorize Information Accessibility

The accessibility of information measures how important it is to have it available when needed. Accessibility should be rated on at least three levels such as critical, routine and archival. In conducting this assessment, the ability to obtain the information from alternate sources must be considered.

4.2.4 Other Information Processing Assets

The steps outlined here for assessing data losses are similarly applied, where appropriate, to losses of hardware, software, source code, system documentation and other key elements of the information processing environment.

4.3 Risk Assessment

The risk assessment component is done by identifying the potential threats to the agency's information processing environment and estimating the probability that the threat will occur. Risks and hazards to the information processing environment arise from many sources and vary widely in probability of occurrence.

4.3.1 Identify Threats

Sources of potential hazard to the agency information processing environment must be identified. Destruction or damage can occur through mistaken or malicious actions of staff, of individuals outside the organization, or by action of natural events. At a minimum, the common threats listed below must be considered. Actual conditions at the agency will determine whether additional factors should be considered.

(1) Human Threats: willful or accidental damage by staff, maintenance workers, visitors or others, sabotage or terrorist acts, loss of key personnel, inexperienced or untrained staff, introduction of viruses, hacking, fraud;

(2) Environmental Threats: power loss, heating, ventilating or air conditioning outages, communications loss, equipment, plumbing or structural failure, release of toxic substances.

(3) Catastrophic Threats: water, fire, weather related, cataclysmic events.

(4) Year Date Threats: Year 2000 and other year date related programming.

4.3.2 Estimate Likelihood of Occurrence.

The probability of occurrence for each identified threat must be estimated. The estimation need not be mathematically exact. A three level scheme (high, medium and low) is sufficient for planning purposes.

4.4 Vulnerability Assessment

Once the risks are assessed, the agency's vulnerability to the risks is evaluated by matching them against the agency's existing internal controls and procedures. In each case the agency must evaluate, considering the importance of the information, its value in terms of initial outlay or replacement cost, and the estimated risk level, the adequacy of the protection in place and decide whether or not it is inadequate, sufficient, or excessive. Risks for which no controls currently exist or for which controls are deemed insufficient, must be identified, and added to the information protection plan. This process may also identify instances where agencies can reduce controls and procedures because the importance and risk do not warrant the resources that have been devoted.

5.0 THE INFORMATION PROTECTION PLAN

After completing the internal control environment assessment, the agency is in a position to develop an information protection plan. The information protection plan establishes both broad general policies and the day to day internal controls, procedures and practices agencies must implement to safeguard the information processing environment against the risks and vulnerabilities identified in the assessment phase. The most effective plans are comprehensive, covering all aspects of the information processing environment and are in written form. Written plans are necessary to facilitate dissemination, provide future reference, and document the agency's efforts.

5.1 Underlying Plan Guidelines

An effective information protection plan reflects the agency's business requirements and specific situation, emphasizes information protection, is cost effective, and has provisions for maintenance and enforcement.

5.1.1 Emphasis on Information Protection

Although the computers, networks, printers and other equipment associated with information processing systems typically become the focus of security and protection efforts, agencies must recognize that the agency's data and information are the ultimate focal points of the protection plan.

5.1.2 Cost Effectiveness

The importance of the business function or the information is the controlling factor in determining the cost to be incurred on protection efforts. Consequently, the cost of security, recovery and other protective measures cannot be inappropriate in relation to the value of the data, systems or equipment being protected.

5.1.3 Maintenance and Enforcement

Plans cannot neglect to incorporate:

(1) Adequate measures, including periodic audits, reviews and surveys to monitor the operation of the information protection plan.

(2) Appropriate disciplinary actions for failure to comply with the plan's procedures.

5.2 Information Protection Plan Organization and Content

5.2.1 Plan Organization

An effective information protection plan's organization:

(1) Clearly identifies the data, information, systems, software and equipment that comprise the agency's information processing environment.

(2) Shows the result of the agency's assessment of the risks and vulnerabilities for the items in (1); and

(3) Enumerates the control activities and procedures that the agency has in place or must implement to protect against the risks and vulnerabilities.

5.2.2 Plan Content

The key elements of a comprehensive information protection plan include:

(1) A general policy statement that emphasizes the agency's commitment to its information protection program and is a clear declaration of the agency's information protection goals and general course of action.

(2) A statement of its scope and purpose.

(3) Identification of the facilities, systems, and personnel to whom it applies.

(4) A discussion of the importance of information security and how it supports the organization's overall goals and responsibilities.

(5) A description of the objectives of information security and the methods for achieving it.

(6) Definitions of violations and penalties for noncompliance.

5.3 Control Activities and Procedures

Sections 6.0, *Organizational and Personnel Controls,* 7.0, *The Physical Environment,* 8.0, *Software Based Controls,* 9.0, *Operational and General Controls,* 10.0, *Business Continuation (Disaster Recovery Plans)* and 11.0, *Monitoring Performance and Results*, of this Directive provide greater detail on specific internal controls, security measures and other practices and procedures that agencies must incorporate, as appropriate, into their information protection plans.

5.4 Additional Information

Risk assessments, policy development and information processing environment protection activities are covered in NIST's September 1996 publication, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, and in the July 1997 draft, *User Guide for Developing and Evaluating Security Plans for Unclassified Federal Automated Information Systems,* issued by NIST's Federal Computer Security Program Manager's Forum.

PART II: INTERNAL CONTROLS FOR INFORMATION PROCESSING ENVIRONMENTS

6 ORGANIZATIONAL AND PERSONNEL CONTROLS

The proper staffing and organization of the information processing environment is an essential element of strong internal controls and a key component of the information protection plan. Proper internal controls require that staff with appropriate training, qualifications and experience be assigned to each function, and that duties and job responsibilities be adequately segregated.

6.1 **Staffing the Information Processing Environment.**

This section briefly describes the primary functions that can play a role in information processing environment management, operation and protection. The degree to which an agency must commit staff resources to data processing will vary depending on the size, nature and complexity of the agency's information processing environment, the extent to which the agency's business operations rely on electronic information and data processing systems, and the sensitivity of the agency's electronic data. The staff for these functions is drawn from various parts of the organization, not just the computer services area.

6.1.1 Planning, Oversight and Monitoring

Information processing environments require a variety of planning, oversight, and monitoring functions. Agencies should insure that staff, and where appropriate, executive and senior management, are assigned explicit responsibility for these functions:

(1) Developing short and long term strategic plans;

(2) Preparing and disseminating agency information protection policies, standards, and procedures;

(3) Developing and communicating security education and awareness programs;

(4) Establishing and monitoring physical security;

(5) Administering systems security and access authorization functions;

(6) Management response to security violations;

(7) Creating, maintaining and testing the business continuation plan;

(8) Auditing all functions, activities and controls.

6.1.2 Data Processing Operations

This function includes the day to day operation and maintenance of all computer resources including hardware, software, networks and telecommunications. It provides the technical and support processes necessary to run a computer in its intended environment to perform its intended functions. Operations have the first level of responsibility for protection of the information processing environment and play a key role in most information protection plans.

6.1.3 Systems Software Support and Maintenance

This function, which is an important specialized activity within data processing operations, is responsible for insuring that the various software that operates computer systems operates correctly and is adequately maintained. Functions include insuring that system software is loaded and running, keeping systems software upgraded, testing enhancements or changes as needed, maintaining system security tables, establishing and maintaining system recovery processes, performing routine backup and retention, and monitoring system performance.

6.1.4 Applications Software Maintenance and Development

The applications maintenance and development function is responsible for maintaining, upgrading, replacing, changing or enhancing existing software applications, and for developing new automated processes or computer systems. This function consists of two distinctly different skills; the analytical component that defines requirements for business changes, and the programming component that converts the business requirements to computer programs.

6.1.5 Internal Audit

The internal audit function examines and reports on the effectiveness of the information protection program, the various levels of controls and security over the agency's systems and on the degree that agency staff comply with agency policies and procedures. Annual internal audits covering all aspects, or major components, of the information protection plan will provide an adequate level of review in most cases.

6.2 Organizing Staff and Segregation of Duties in the Information Processing Environment

The information processing environment, like most aspects of agency business, benefits from the appropriate segregation of employee duties and responsibilities. Because data processing concentrates many functions that, prior to the advent of automation, were performed manually by different individuals, information processing environments provide many opportunities for fraudulent or collusive manipulation of data and programs and destructive acts. Proper internal controls dictate that agencies adequately segregate duties to insure that individuals with knowledge and technical skills do not have inappropriate access to agency business functions, and adequately separate duties within the data processing technical environment. The segregation of responsibilities to allow for as much separation of sensitive functions as possible without unduly sacrificing efficiency is a critical organizational issue.

6.2.1 Segregation From Accounting and Business Functions

The proper segregation of data processing staff from accounting and business function requires that:

(1) The information system/data processing department is organizationally separate and independent of the accounting department.

(2) The information systems/data processing department is separate and independent of any organizational unit for which it processes data.

(3) The data processing area be physically separated from other organizational units.

(4) Information systems/data processing personnel not be permitted to initiate or authorize routine agency business transactions of any kind.

(5) Information systems/data processing personnel be prohibited from initiating any transaction processing without user authorization.

(6) Applications programming staff do not have access to cash or checks.

(7) Only information services staff operating personnel are allowed access to centrally located computers, network servers or central telecommunications equipment.

6.2.2 Segregation of Duties Within the Information Services/Data Processing Department

To properly segregate responsibilities within the Information Services/Data Processing department, to the extent practicable, the following functions are performed by different individuals:

(1) Systems Analysis. The design of computer programs to meet the objectives of the user departments.

(2) Programming. The preparation of the programs or instructions to be followed by the computer. Includes applications and systems programming.

(3) Machine Operation. Running the computer equipment that processes the data and information.

(4) Librarian. Controlling access to computer software, programs and files.

(5) Control. Insuring the integrity of data received from operating departments (input) and of computer information produced for distribution (output).

6.2.3 Segregation from Monitoring and Audit Functions

In a properly segregated environment:

(1) Internal audit is independent of the information services/operations function and reports to the Agency Head or an executive level manager.

(2) Monitoring and compliance assurance activities are independent of operations and development.

6.2.4 Segregation of Duties in Small Organizations

Segregation of duties is a particularly challenging control to implement in agencies with a small number of employees. It is important that managers in such agencies carefully consider this principle when designing and defining job duties, and remain cognizant of the heightened risk when a smaller number of employees preclude optimal segregation of duties. Techniques for counterbalancing the shortfall in staff include increased surveillance, heightened controls, and an escalation of the management/supervisory level at which reviews are made. Management's close and documented review and approval of transactions, reports and reconciliations become especially critical in small departments with limited numbers of personnel.

6.3 Additional Personnel Security Considerations

The following practices should be implemented where appropriate:

(1) Individuals who have access to sensitive information resources should be subject to special security procedures. More extensive background and reference checks, including Department of Investigation background inquires, may be appropriate for such positions.

(2) Security responsibilities should be explicitly covered in employee orientations.

(3) Position descriptions, tasks and standards, and performance evaluations should explicitly reference sensitive responsibilities that affect the security of information resources, such as password maintenance.

(4) All professional and managerial data processing personnel should be required to take vacations of at least two weeks in length each year.

(5) Individuals in sensitive positions should be subject to job rotation and work flow should be designed in such a way to provide as much separation as possible.

(6) The duties of those individuals who are responsible for the input of sensitive or confidential information should be segregated and distinct from those individuals who are responsible for output balancing and control.

(7) If circumstances warrant such action, an expedited termination or rotation to less sensitive duties for the remainder of employment, and cancellation of access privileges to the system and secure areas, is strongly advised upon a decision to terminate, or receipt of notice of resignation for employees with access to critical data processing resources.

7.0 THE PHYSICAL ENVIRONMENT

Physical security is the most basic and commonly addressed form of information processing environment control. Physical security encompasses safeguarding not only computer facilities and general work areas, but also includes areas where essential support equipment such as air conditioning, communications lines, network and communication hubs, power control panels, and tape/disk storage are housed. Physical controls constitute the first level of defense in the protection of the information processing environment. Protection from vandalism, theft and damage by fire, water, air borne contaminants and loss of power are all elements of physical security.

7.1 Understanding Physical Security Risks

7.1.1 Agency heads must recognize that information processing resources represent physical risks for a number of reasons:

(1) Equipment is sensitive and can malfunction because of environmental factors that are not immediately apparent, or accumulate over time. Examples are airborne contaminants such as dust, temperature extremes and humidity.

(2) Computer resources, particularly storage devices and central processors, concentrate valuable, perhaps irreplaceable, data in a single location making it highly vulnerable to a localized hazard, vandalism or misuse.

(3) Many computer components are expensive, portable and interchangeable making them readily marketable or useable in other situations. As such, they are an attractive target for theft or misappropriation. Examples include laptops, easily removable memory chips, cards, drives, cables, boards and other components of desk top computers.

7.1.2 Insuring adequate physical controls starts with an understanding of the nature of the equipment and its use and of the physical space where the equipment is housed or used. Generally, equipment falls into three broad categories:

(1) Central, core equipment. This equipment is generally housed in rooms, offices or cabinets that are easily separated from the general population and are accessible to a limited group of employees. Examples include central processors, servers, mainframes, and mass storage devices.

(2) Distributed equipment that is assigned to individuals or shared by a group generally located in offices that are accessible by the general population. This category includes PCs, printers, readers and other office based equipment.

(3) Off-site equipment. This is a subset of distributed equipment, but because it is taken off the agency premises, is more difficult to secure. Examples include, laptops, radio based equipment, digital cameras and scanners.

7.2 General Physical Security Controls

A number of underlying principles apply to all or most equipment:

(1) It should be kept in a clean, dust free and smoke free environment. Dust can clog equipment heat vents. Dust and smoke particles can accumulate on drives, disks and other parts causing malfunctions. Often the impact is not immediate, appearing suddenly after weeks or months.

(2) Computers generate large amounts of heat which, if allowed to build up can cause damage and failures. Computer spaces, particularly where central equipment is located, must be adequately climate controlled to insure that temperatures remain within the operating range specified by manufacturers. The electronic components in computer equipment are also sensitive to excess humidity. Again, humidity must be kept within the limits specified by manufacturers.

(3) Protection from electrical power problems. Computer equipment is easily damaged by the spikes or surges in electric power that are frequently transmitted through power lines and electrical supply systems. If the location's overall power supply is not power conditioned, all equipment should be connected to surge suppressors. Core or critical equipment must be further protected by uninterruptable power supply (UPS) units, which keep equipment running, and/or shut it down in an orderly fashion, when electric power is cut off for any reason.

7.3 General Office Security

Because it is not feasible to closely monitor general office space where information processing resources are located, physical controls are more difficult. Agencies should consider all or any combination of the following to the degree practicable:

(1) Limiting the number of ingress and egress points.

(2) Stationing a receptionist at the entry point.

(3) Not allowing members of the public or strangers free or unattended access to the office.

(4) Insuring that doors and windows are locked overnight, during lunch hours, etc., and restricting the issuance of keys to the degree possible.

(5) Use of security guards

(6) Package inspection

(7) Requiring the immediate reporting of, and prompt follow up and investigation of missing or vandalized equipment incidents.

(8) Conducting regular physical inventories of distributed equipment components and software and following up on all discrepancies.

7.4 Specialized Physical Security for Controlled Access Areas

Controls for limited access spaces housing the agency's most sensitive equipment, typically a computer room, data center or hubsite, include:

(1) Entry restriction only to authorized personnel. Available systems vary greatly in sophistication, ranging from simple key card, to biometric access devices, some can deny access to even authorized personnel during specific periods, some can record the identity, for later review, of all persons entering and leaving, some will sound audible intruder alarms.

(2) Humidity and temperature detection devices with alarms, smoke detectors.

(3) Fire extinguishing systems.

7.5 Network Components

In distributed architectures, certain equipment not housed in computer rooms can represent a point of failure because an outage would affect a significant segment of the user population.

(1) Distributed network equipment such as concentrators, routers, file servers and other equipment not kept in centrally located equipment or wire rooms must be located in protected space, locked cabinets, or other environments which cannot be accessed by unauthorized individuals.

(2) Network wiring, especially backbones, should be run in protected chases to reduce exposure to unintentional or malicious risks.

7.6 Inventory Control

A key element of physical security is the careful inventorying of all agency hardware and software. Agencies must maintain detailed inventory and accountability reports for all physical assets in the information processing environment.

The PC equipment component of the inventory represents a special problem because of the large number, wide distribution and continuous flux of the equipment and because of the many subcomponents in personal computers. RAM, and other components, for example, are interchangeable and subject to theft. Similarly, the loaded software can change continuously. Although difficult to establish and maintain, an accurate inventory is a highly useful management tool that serves a variety of accounting, administrative and other management purposes including use in verification that City property is accounted for and for developing maintenance schedules and support strategies. The PC inventory details can provide significant benefits in administering networks by helping to establish standard profiles.

Maintaining an accurate inventory requires that agencies insure that inventory data is kept updated on an ongoing basis by carefully controlling additions, deletions and changes to installed equipment, particularly PCs. Additions, deletions and changes must be promptly posted to the inventory records. The disposition of all equipment removed from service must be recorded. Physical inventories should, at a minimum, be conducted annually to insure that actual equipment matches the inventory records. All discrepancies must be resolved.

7.7 Laptop Security

Laptops and other electronic equipment that frequently leave the agency's office environment introduce special control problems due to their portability and high unit cost. A clear written policy covering laptop assignment and use, and physical verifications of the laptop inventory, taken at least once a year, are necessary to insure the protection and control of laptops.

A comprehensive laptop security policy contains procedures to insure that:

(1) When not in use, laptops are stored in a secure, locked location.

(2) Laptops are never left unattended when in transit.

(3) Only agency owned and authorized software is used on laptops, the use of personal software, free software and vendor demos is prohibited without prior agency authorization, and illegally copied software is never used.

(4) Only agency owned and approved hardware is used in conjunction with laptops.

(5) Laptops are never connected to any computer system unless approved first by the agency information services staff.

(6) Access to the agency LAN is only via an appropriate method that ensures proper security.

(7) All software and/or data is scanned for viruses before loading onto a laptop

(8) Laptops are scanned for viruses before and after any connection to the agency LAN.

(9) Laptops with agency sensitive data are protected by an access control password.

(10) Only agency business is conducted on the laptop and only agency staff uses it.

(11) All applications are backed up regularly.

(12) Diskettes and sensitive files are removed before return to pool.

8.0 SOFTWARE BASED CONTROLS

There are many software based controls that can be employed to help protect the information processing environment. Software based controls, also referred to as logical controls, consist of a variety of features that are programmed into software. The features help managers define and control access to computer systems, specific data or functions within systems, and system hardware.

Principal software based security capabilities include:

(1) Control of the individuals who are authorized to access information systems;

(2) Restriction of individuals' access to specific data or resources; and

(3) Creation of computer generated audit trails of user activity.

8.1 Access Control Software

Access control software is designed to permit management to control who accesses information system resources. It automatically identifies and authenticates individual users to the system, and enables the system to create a record or audit trail of access related events for later review and investigation. Access control can either be provided by separate programs built into operating or applications software, or by an independent product that is integrated into the environment.

8.1.1 General Access Controls

General access control software, which secures the entire information processing environment, is preferable; however, its use may not be possible in all environments. In such cases, agencies should employ the individual access control features provided with the various software products in use. Operating systems, library and database management systems, teleprocessing monitors, telecommunication systems and utilities are examples of software that generally have built in security features.

To insure that general access controls are effective, agencies must analyze system access paths and control points. An access path is the route by which someone can gain access to the system. The analysis of access paths must be done carefully, because access can often be achieved indirectly through a multi step path. A control point is a strategic point on an access path that may be used to control system access. The control points on each access path should be identified.

A simple access control is the use of a time out feature that automatically logs off an end user workstation if no activity is detected after a pre-specified time.

8.1.2 Access Control - User IDs/Passwords

User identifications and passwords are among the most widely used and visible forms of access control. The user identification identifies the individual to the system. Passwords control the applications or system information an individual is permitted to access. Access authorization must be carefully designed to insure that employees have access only to files or programs that are necessary for their job function.

Active password management includes:

(1) Insuring that users are forced to change passwords periodically;

(2) Limiting the reuse of passwords;

(3) Deactivation of inactive user accounts and accounts for employees whose services have terminated; and

(4) The dissemination of a written policy that provides user guidance for protecting the integrity of passwords.

8.1.3 Access Control - Personal Computers (PC)

Information stored on a local PC hard disk or laptop, is subject to hazard even if access control or other software is installed. Hard disks can easily be removed by an unauthorized individual, and inserted into an unprotected PC, enabling access to the protected files or applications. Because of the nature of the PC operating system, special attention must be taken to ensure that, upon "deleting" a file, files are fully erased rather than simply deleting the storage address.

8.2 Application Software Controls

Application software controls are automated controls built into application programs. They ensure that every transaction entering the information processing environment is authorized, recorded and processed completely and accurately, protected from physical loss, theft or unauthorized manipulation and that the data file integrity is preserved. Agencies must insure that adequate application controls are in place to eliminate the input, processing and output risks discussed here. Only authorized employees should have access to application control software.

There are a variety of application controls:

(1) Data origination controls are designed to ensure that data is accurate, complete and timely when it is entered into the processing system. These controls insure that data stems from approved sources, is properly authorized, that input errors are properly handled and that documents are retained if necessary.

(2) Input controls are designed to ensure accuracy, completeness and timeliness of the data when it is converted to the electronic format readable by the agency's information processing systems. Input controls cover data entry, data conversion, data validation, editing, and error handling.

(3) Data processing controls ensure complete and accurate transaction processing in the proper period or cycle. Data processing controls, which help insure the integrity of data processing within the application, include data validation, editing, error handling, and the identification and processing of rejected transactions and suspense items.

(4) Data output controls help ensure the integrity of application outputs. These include output balancing and reconciliation, error handling, output distribution, and retention.

(5) Backup and recovery controls can be used to mitigate any system failures or processing disruptions that may occur. These controls may include journal logs, transaction files, before and after images of databases, recovery/restart software, and shadow file processing.

8.3 System Software Controls

System software controls are automated controls generally supplied by vendors as a component of their software packages. System software, as opposed to application software, consists of operating programs and other programs or systems that monitor or help interconnect, coordinate, and direct the various elements of input/output, processing, data storage and application processing. System software controls are found in:

(1) Operating system software, which is an integrated set of specialized programs used to manage the resources and overall operations of a computer, including control of application programs, files, and other resources;

(2) Database management systems, which handle the tasks associated with creating, accessing and maintaining database records;

(3) System monitors that assist in troubleshooting and diagnosing equipment malfunctions;

(4) Network controllers used to supervise and control transmissions between host computers and peripheral telecommunications devices;

(5) Teleprocessing monitors that support interactive, on-line communication between terminals and the host computer;

(6) Job scheduling software, used to manage and control production schedules in the computer room;

(7) Job accounting software, used to monitor, measure, and document computer resource usage;

(8) Library management software, used to control the storage and use of application programs;

(9) Tape/DASD/disk management software, used to control the use, distribution, and disposition of tapes, cartridges, optical disks, and DASD;

(10) Performance monitoring software, used for tracking response time and CPU utilization;

(11) Utilities that perform system services, such as managing disk space; and

(12) Capacity planning software, used to analyze computer workloads.

8.4 Software Viruses

Software viruses are invasive computer programs that can severely disrupt information processing environments. Once introduced into a networked system, a virus can rapidly spread to all users' PCs, routers, file servers and central processors.

Viruses take many forms. Some malicious types can perform destructive acts such as erasing files, altering stored data or gobbling up free storage space. Others are annoying but not destructive. Once a virus becomes entrenched, it can be a labor intensive, time consuming effort to completely remove it from the system.

Protection against software viruses requires a combination of software based and procedural access controls:

(1) Avoidance. Entry of a virus is possible whenever files are transferred into the agency's system from an outside source. Laptop computers are a frequent entry point. Other entry points, including diskettes or downloaded files received from non-agency sources, including the Internet, must be scanned to eliminate potential viruses.

(2) Early Detection and Isolation. Once a virus has been introduced, the less time it has to spread, the easier elimination is.

(3) Virus Detection Software. This software must be installed on agency LANs, LAN attached and stand-alone PCs, and, because new viruses are created continuously, must be constantly maintained with current updates. Virus detection software should check for viruses upon login and periodically during the day.

(4) User Education. The dissemination of a written policy that educates the user community on methods for avoiding the introduction of viruses, and requests their assistance in the early detection of virus activity.

(5) Response Plan. A formal response plan that can quickly be put into action when a virus is detected.

8.5 Audit Trails

A key element in the control over the information processing environment is the incorporation of audit trails into general and application control procedures. Audit trails

maintain records of a variety of system events and activities. Every data entry or change, all modifications of system software or application software, and changes in the authorized use of a system's physical resources should result in the recordation of the event so that management or auditors can trace any change back to its source.

8.5.1 Audit trails can provide a means to help accomplish the following security-related objectives:

(1) Individual Accountability. Audit trails provide a record of user actions enabling management to review or verify user activities.

(2) Reconstruction of Events. Audit trails enable after-the-fact investigations of how, when, and why problems occurred.

(3) Intrusion Detection. If properly designed, audit trails can assist in intrusion detection in either real time, or after the fact.

(4) Monitoring. Audit trails may be used as on-line tools to help identify problems other than intrusions as they occur. This is often referred to as real-time auditing or monitoring.

8.5.2 At a minimum, the audit trail should:

(1) Record the user ID associated with the event, date and time information, session data and program and file usage.

(2) Cover all components of the network (e.g., workstations, servers, and infrastructure).

(3) Summarize and report audit data daily, particularly key information such as security violations

(4) Have adequate access controls such as encryption of log file data and strict assignment of access rights, to prevent the alteration or disabling of the log by users and administrators.

8.5.3 It is important that the agency's procedures delineate the individuals or group responsible for, and frequency of, the review of audit trail data. Audit trails should be reviewed regularly, and exceptions followed up. Automated analysis tools should be used where practicable.

8.6 Computer Hackers

Computer hackers can be either internal staff or persons from outside the organization who intentionally, or maliciously, attempt to gain unauthorized access to the organization's information processing environment for malicious, destructive or fraudulent purposes or just for entertainment and unauthorized browsing. Hackers intrude, not only for information, but also to use system resources such as bandwidth, storage, and CPU. Hackers can gain access through a variety of paths, including dial in, the Internet, central core equipment, or unattended workstations. Although unauthorized users may gain system access through an opening in either physical or logical system security, hacking generally refers to the latter.

Hackers may attempt to gain access through the trial of common or vendor supplied passwords, use of speed-dial configurations or the interception of passwords/access codes retrieved from Internet "sniffers" or public dial-in systems.

The risks associated with computer hacking include:

(1) the disclosure of confidential organizational data.

(2) the destruction or alteration of critical organizational data.

(3) the introduction of a virus or worm into the network.

The risk of a system being hacked can be minimized by implementing and maintaining the general access and application controls and security discussed elsewhere in this section.

9.0 OPERATIONAL AND GENERAL CONTROLS

This section covers a variety of security, operational and control issues that cannot be categorized as either purely physical or software based controls. These controls must be included in the agency's information protection plan as appropriate.

9.1 General Network Management and Security

This paragraph covers a number of issues primarily associated with LAN and WAN management.

9.1.1 The objectives in securing networks include:

(1) Maintaining the confidentiality and integrity of data stored, processed or transmitted across the network

(2) Maintaining the availability of data stored on the network

(3) Maintaining the ability to process and transmit data in a timely fashion

(4) Ensuring the identity of the sender and receiver of each message

9.1.2 Security mechanisms, procedures and other controls used to mitigate network vulnerabilities and threats include:

(1) Identification and authentication of users to help ensure that the network is accessed by only authorized individuals

(2) Access control to ensure that network resources are being utilized in an authorized manner

(3) Data and message confidentiality to ensure that network data, software, and messages are not disclosed to unauthorized parties

(4) Data and message integrity to ensure that network data, software, and messages are not modified by unauthorized parties

(5) Non-repudiation of communication whereby the entities involved in a communication cannot deny having participated in it

(6) Logging and monitoring uses of all network resources

(7) Dial-up facilities must install and use a secure dial-back technique before entry is gained to the network by authorized users who dial in from remote locations.

9.1.3 Internet and Other Network Access Paths

Network access paths such as Internet connections, telephone lines, and other communication links pose a number of security issues for agencies. The most problematic risk is that these points are potential access paths for unauthorized entry into agency computer systems. Skilled computer hackers, for example, can use the Internet to access data files, introduce viruses, or install a "sniffer" that can capture user passwords and other authentication information which may then be used to access agency systems.

For all networks, especially those connected to the Internet, managers should implement and maintain the following procedures:

(1) Identify and maintain an updated list of all network entry and exit points. Security software tools are available to develop and maintain such lists.

(2) Install firewall software at all entry and exit points to control and track access to the network. Firewalls must be periodically reviewed and updated to meet the ever changing threats from external sources.

(3) Use operating system and other software patches and updates whenever they include fixes to known system vulnerabilities.

(4) Use physical and software system monitoring and intrusion detection features (such as port scan detection software) to identify any unauthorized network probing or intrusions.

(5) Treat all software downloaded through the Internet as potentially virus laden and insure that it is thoroughly scanned for viruses with up-to-date virus detection software.

(6) Employ data encryption and one-time passwords when data communications are particularly sensitive, such as in the transmission of credit card information.

(7) Separate web servers from LANs and other systems.

All agencies are encouraged, and Mayoral agencies are required, to follow the existing guidelines or subsequent directives issued by the Mayor's Office and DoITT. The guidelines in effect as of the issuance of this Directive are listed in Appendix A.

9.1.4 Electronic Mail

The advent and widespread use of electronic mail raises a number of internal control and policy issues for agency management. Existing telephone, fax or written communication policies may serve as useful models for an electronic mail policy, however, these policies will need to be tailored to meet the unique characteristics of e-mail. For example, files attached to e-mail from external sources should be checked for viruses. The responsibility for developing and monitoring e-mail use and policy will generally be a collaboration between agency legal, data/information administrators, and records management staffs.

To adequately protect electronic mail as an agency asset, e-mail policies should contain the following elements:

(1) Roles and Responsibilities

Clarifies the responsibilities of managers, network administrators, technical staff and end users.

(2) Appropriate Uses of Electronic Mail

Establishes limits on personal use similar to those that exist for postal mail, phone or fax. The policy should recognize that although some personal communication is likely, e-mail's fundamental function within the Agency is to support official business. Given the dual nature of electronic mail: immediate and informal like a phone call, but irrevocable like a memorandum; staff must be made aware of their responsibility for the content and potential future dissemination of their messages.

(3) Access and Privacy

Informs e-mail users to have a limited expectation of privacy protection regarding any and all e-mail communications sent or received, and states that e-mail messages sent or received:

(a) Can remain on servers and back-up tapes indefinitely, even though deleted by the employee;

(b) May be accessed and monitored by management, system administrators, supervisors or other appropriate persons;

(c) Are subject to discovery proceedings in legal actions;

(d) May be releasable to the public under the Freedom of Information Law (FOIL);

(e) May require special measures for privacy protection to comply with the Personal Privacy Protection Law (PPPL).

9.1.5 Additional Information

FIPS PUB 191, *Guideline for the Analysis of Local Area Network Security*, (November 1, 1994), provides detailed guidelines for the protection of LANs and PCs.

9.2 System Backup and Recovery

It is essential that agency policy and procedures insure that backup and recovery procedures are in place for applications and operations software, files and data bases. To recover from accidental or deliberate destruction of software and data, frequent system backups are essential and should be made a part of regular operations. Complete system backups should be taken at intervals determined by how quickly information changes or by the volume of transactions. Backups should not be stored in the same location as the operational data to guard against the possibility of original and backup copies being destroyed by the same event or incident.

9.3 Applications Software and System Software Change Control

A change control policy is necessary to insure that only appropriate, authorized changes are made to application and system software. Changes can range from the rectification of minor bugs to module replacements and major enhancements. Major changes should be undertaken with great care. They involve considerable time, effort and agency resources, and could adversely impact existing systems. Periodic reports describing the changes underway and the progress toward implementation should be provided to executive management.

9.3.1 Change Control Program

Elements of a change control program include:

(1) A formal approval and review process that ensures that changes to application and operating system programs and data are not made unless explicitly authorized by appropriate agency personnel.

(2) The process must identify the source of the change request and must require approval at sufficiently higher levels of authority depending on the scope of the change requested.

9.3.2 Internal Control Techniques for Software Changes

Close controls over software changes are essential to maintain continuity and reliability. Key control principles include:

(1) Minimizing the effects of the introduction of new code in a production environment;

(2) Making and testing software changes in a test environment;

(3) Testing critical applications with the modified system software;

(4) Acceptance testing modified software in the production environment.

(5) Obtaining technical services management's authorization before changes are made to system software;

(6) Allowing only authorized personnel to perform modifications;

(7) Fully documenting the modification process including the identification of the exact feature being modified or implemented;

(8) Limiting and controlling the number of "user exits" when modifying software;

(9) Limiting and controlling modification from remote sites; and

(10) Use of formal change control procedures for all software updates.

9.4 Problem Management Control

The establishment of a central problem control function is a technique that is used to identify, monitor and resolve information processing environment operational problems. Problem control techniques are necessary for hardware, communications software, network, production processing, applications software and operations. This function should:

(1) Document reported problems.

(2) Identify the specific cause of the problem.

(3) Develop a plan for resolving the problem.

(4) Monitor progress at correcting the problem.

(5) Verify that the problem has, in fact, been corrected.

(6) Maintain a problem history file.

(7) Periodically report repetitive, unresolved problems to executive management.

9.5 Systems Development Methodology

Agency management must be alert to a variety of management and internal control

issues when undertaking the development of new computer systems or making major changes to existing systems, using either in-house resources or external system development and integration services.

The development of major computer systems is an expensive, time consuming and resource intensive undertaking. System development projects, by nature, are technically and organizationally problematic, and prone to a number of risks that can result in runaway costs, extended development periods, failure to meet the initial needs and objectives, and, in the worse cases, outright failure.

9.5.1 System Development Controls

There are a number of internal control techniques that can help agencies insure the success of system development projects.

(1) Obtain executive management support and active sponsorship;

(2) Involve end users in the specification of system requirements;

(3) Use an experienced project manager to oversee and coordinate the process;

(4) Employ skills transfer techniques to insure that agency technical staff can adequately support the completed system;

(5) Follow a formal system development methodology to manage the development process;

(6) For very large and/or highly critical projects, engage an independent quality assurance consultant to assist the agency monitor and review the work of the development and integration team.

9.5.2 Major System Development Components

The risks inherent in agency systems development projects can be significantly alleviated by conducting them in accordance with a formal systems development methodology. Such methodologies help insure that system development efforts are conducted in a structured, logical, organized, and efficient manner and help insure that systems meet their objectives, and are developed within budget and time constraints.

Typical steps include:

(1) Systems Requirement Definition

(2) Technical Design

(3) Programming

(4) Conversion

(5) Testing

(6) Implementation

(7) Post Implementation Support

Following a formal methodology further insures that work steps and deliverables are authorized, approved, and documented.

9.5.3 Internal Controls for New Systems

The orderly development of new systems and applications play a role in information protection, because the incorporation of appropriate internal controls must be part of the development process for new systems. Common approaches to security threats can be implemented to ensure robust system responses to attempted violations.

9.6 Communication of Policies and Procedures

To be effective, information protection policies and procedures must be communicated to agency staff and must convey the agency head's recognition that information protection is an important agency objective.

(1) Policies should be posted conspicuously and redistributed to employees frequently to emphasize their importance to the agency;

(2) Policies should be reviewed and updated periodically, but no less than biennially.

9.7 Computer Operations Documentation

In sound internal control environments:

(1) Agency information processing functions are governed by written procedures that document the operation and maintenance of the equipment, systems and networks;

(2) Management insures that operational staff has access to the operations

documentation, is adequately trained in its use, and that the documentation is reviewed and updated periodically; and

(3) Changes to documentation are controlled to insure that they are made only by authorized personnel.

Documentation requirements include: system input and output controls, scheduling jobs and activities, malfunction reporting, backup and recovery procedures, preventive maintenance, file and library management, operational security, maintenance of operating system configuration tables, systems software output that can be used for review and that provides an audit trail; and the business continuation plan and disaster recovery process.

9.8 Unauthorized Activities

Agency policies and procedures should require, that, like other agency resources, information processing resources, including PCs, laptops, and the Internet, are to be used only for official business and are not to be used to make discriminatory, harassing, or libelous communications. Agencies should communicate to staff that they can review saved files at any time and that appropriate disciplinary action will be taken for prohibited uses of computing resources.

9.9 Copyright Infringement and Intellectual Property Policy

It is a violation of federal law to make copies of software without the express permission of the company that licenses the software product. Agencies must have a written policy covering the illegal copying or pirating of software and software documentation.

At a minimum, a copyright infringement policy:

(1) Clearly states that it is illegal to make unauthorized copies of software products for any reason.

(2) Prohibits employees from copying agency software for use elsewhere in the agency or for personal use.

(3) Prohibits employees from loading illegally copied software on agency equipment.

(4) Requires that agency usage of software products does not exceed the number of licensed copies owned.

10.0 BUSINESS CONTINUATION (DISASTER RECOVERY) PLANS

A formal plan for the recovery of agency operations and the continuation of business after a disruption due to a major loss of computer processing capability is an important part of the information protection plan. The increasing dependence on computers and data processing support makes it ever more critical for Agency Heads to focus on this area.

10.1 Business Continuation Plans - General

Business continuation planning prepares for events that exceed the ability of the routine back up and operations recovery procedures that handle day to day, short term and localized outages. They map out the agency's response to the kind of major, very infrequently occurring events that are of such a magnitude that they cause the loss of, all, or major segments of, the agency's operations over a sustained period of time.

The business continuation plan, also called a contingency plan, or disaster recovery plan, enumerates the steps the agency will take to recover computing operations. Plans can vary widely in their breadth and scope. The most basic may consist of actions that maintain an agency's "presence" during a comprehensive loss of computing resources, simple procedural changes, or provision for manual processing and workarounds. More elaborate plans may be geared to promptly reestablishing business temporarily at alternate locations, through emergency vendor supply arrangements, reciprocal service agreements, disaster recovery site, or service bureau arrangements.

In developing business continuation plans, agencies must consider separately scenarios involving the loss of a data center, satellite office, or other critical points of failure in the agency's information processing environment.

10.2 Cost Justification

Depending on the size, complexity and criticality of the agency's information processing environment, effecting business continuation arrangements may require substantial effort and significant cost. Costs for the most "seamless" plans can be extremely high, requiring careful consideration of the cost benefit principle discussed in §5.0, *The Information Protection Plan.* Consequently, business continuation plans must reflect an assessment of the impact that a major system interruption or loss would have on the agency's operations and the degree that the agency is willing to accept such risk.

Much of the impact assessment should have been conducted as part of the internal control assessment described in §4.0, *Assessing the Internal Control Environment.* The

impact assessment must consider the duration of the outage. For example, agencies may find that a short outage requires no contingency plan, but a loss that lasts more than two, five, or ten days does.

Impact is measured in terms of both cost and non-financial implications. The cost of a major system interruption includes losses due to idle staff and equipment, and ongoing costs such as maintenance and service contracts, as well as the incurrence of additional expenses such as interest costs, fines, suits, and "catch up" processing costs such as overtime. Non-financial costs include loss of public confidence and stoppages or delays in providing services to the public, the impact on other systems that depend on the agency's systems, and the failure to meet legal requirements.

10.3 Recovery Plan Components

The primary elements of a business continuation plan include:

(1) The steps the agency will take to determine whether or not an event is sufficiently serious to invoke the plan.

(2) Responsibility assignment. The names, telephone numbers and specific responsibilities of each individual in a disaster situation.

(3) A pre-arranged agreement describing the conditions under which a disaster is to be declared.

(4) Specific procedures. These can vary greatly depending on the degree of the disaster event. Dependencies include: the parts of the agency that can work and the parts that cannot, the length of time the outage is expected to last, the availability of work space and/or staff to do work rounds or manual processing, and the identification of manual processing procedures or workarounds that may be instituted.

(5) Prioritization. Establishes the order of priority in which information systems are to be reinstated.

(6) Equipment and software supply agreements.

(7) Recovery assistance consultants.

(8) Hot site, cold site, service bureau or reciprocal arrangements

10.4 Plan Updating and Testing

Periodic reviews and updates are necessary to insure that the business continuation

plan remains current. A comprehensive test should be conducted annually.

10.5 Network Recovery

If the agency operates a local area or other network, a network recovery component is a critical element of the business continuation plan. Special attention must be devoted to the accurate inventorying of workstation and PC technical specifications, configurations, network software and hardware, network operating hardware and software, and application software.

10.6 New Systems

Disaster recovery is an integral part of the overall plan when designing, specifying and implementing new computer systems.

10.7 Citywide Disaster Recovery Plans

The City's largest and most critical computer systems, including IFMS[1] and PMS, are covered by disaster recovery plans that have already been developed by the Financial Information Services Agency, the Office of Payroll Administration and DoITT. These plans generally cover the loss of the central agency's data processing centers and networks. Whereas agencies may, in part, be covered by Citywide recovery plans, agency heads must understand that these plans generally cover systems and databases of Citywide importance and do not cover agency based equipment, networks and data, or systems developed by the agency.

If an agency receives services from a data center it doesn't own or operate, the agency must insist that the service bureau has an adequate business continuation plan, must insure that it is tested annually, and must incorporate the service bureau's plan as an integral part of the agency's business continuation planning. Similarly, if the agency uses, but does not operate, a local area or other network, the network operator must provide access to the network recovery plan for review purposes.

10.8 Additional Information

Business continuation and contingency planning is covered in FIPS PUB 87, *Guidelines for ADP Contingency Planning.*

[1] [Effective July 1, 1999 the Financial Management System (FMS) replaced IFMS.]

PART III: MONITORING PERFORMANCE AND RESULTS

11.0 MONITORING PERFORMANCE AND RESULTS

A critical part of the agency's internal control environment is the establishment of a set of procedures and techniques designed to monitor the adequacy of the information processing environment's performance and insure that it is reported to the level of management that has the authority to insure that corrective action is taken. Implementing performance monitoring techniques will help agency management routinely assess the effectiveness of the agency's control procedures in achieving the information processing environment's operational objectives.

Insuring that problems, security breaches, poor performance and other significant events impacting the information processing environment are regularly and frequently reported to executive management will help management focus on the remediation of control and operational weaknesses. Summary level reporting in each of these areas will provide a snapshot of information activities and will enable agency executive management to better understand the state of the information processing environment in their agency.

11.1 Downtime Reporting

Downtime reports alert management to the amount of time that information processing resources were unavailable for agency staff use. Downtime reporting includes regular summary reports that describe system operational results, with particular emphasis on the level of service provided to users. The primary purpose of these reports is to assess the availability of various system components for their intended purpose and to focus attention on the impact on staff productivity.

11.2 Service Level Reporting

Service level reports indicate the number of requests for routine technical assistance, the time taken to respond, the time taken to correct the problem and the unresolved problems. Executive management can use this information to determine if repetitive problems persist, if service to agency staff is meeting agency goals, the adequacy of agency or vendor supplied response resources, and the impact on staff.

11.3 Application Development/Systems Changes

Regular summary level reports describing the number and type of staff requests for new computer applications or changes to existing applications will provide executive management with an understanding of the degree that existing applications fail to meet agency user needs and where in house application development or external system development resources should be applied. The reports should summarize new items

requested, the authorization for any changes undertaken, items in progress, items completed and provide an indication of the time that requests have been outstanding.

11.4 New Technologies

Plans for the purchase and installation of new technologies, including hardware and software, should be reported to executive management. Management needs to insure that the technology is consistent with the agency's information processing policy and long range plan, must understand and be comfortable with the risk factors involved with any new technology, and must obtain assurance that internal control considerations have been adequately addressed before the technology is installed in the agency.

11.5 Security Violation Reporting

A record of the physical and logical security violations detected by software controls and other monitoring procedures must be reported to senior management. The most serious security violations should be reported to executive management. A review of security violations will highlight unresolved problems or weaknesses in internal controls and may show patterns of failure and abuse requiring remedial action.

11.6 Internal Audits

The agency's internal audit function should play a supportive role in the review and establishment of internal controls over the information processing environment. Internal audits can alert management to lapses in compliance with internal controls, the need for new or revised controls and other issues that should be brought to management's attention. To insure independence, internal auditors report directly to executive management.

11.7 Inventories

The results of periodic inventories and the actions taken to account for discrepancies must be reported to management. Patterns of repeated losses and reconciliation problems indicate internal control weaknesses that must be rectified.

11.8 End User Comments

Periodic commentary from end users is an effective method that executive management can use for assessing information processing environment performance. Satisfaction reports from the end user community will frequently highlight common or recurring problems requiring executive management's attention. These reports are most useful if they flow to executive management independent of the information systems group.

11.9 External Assistance

There are a variety of private sector services that can assist agencies monitor, test and audit the condition of their information processing environments. Many public accounting firms, for example, offer security audit services that will identify weaknesses in an agency's security systems. Agencies may also hire a computer penetration specialist that will aggressively attempt to hack into an agency system to demonstrate holes or lapses in the agency's security environment.

g:/docs\mas_dir\dir#18

APPENDIX A

ADDITIONAL SOURCES AND INFORMATION

This Appendix identifies authoritative organizations and reference materials that agencies can use to supplement the controls, policies and procedures covered in the Directive and to learn more about selected subject areas.

Auditing and Internal Controls

American Institute of Certified Public Accountants (AICPA). Statement on Auditing Standards (SAS) 55, *Consideration of Internal Control in a Financial Statement Audit,* April 1988.

American Institute of Certified Public Accountants (AICPA). *The Auditor's Study and Evaluation of Internal Control in EDP Systems*, 1977. Withdrawn.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). *Internal Control - Integrated Framework*, September 1992.

Institute of Internal Auditors (IIA) Research Foundation. *Systems Auditability and Controls Report*, 1991.

City of New York - Department of Information Technology and Telecommunications

Guide to Systems Security Facilities at CSC, 1994

RACF Guide for the Client Security Administrator, 1994

Guide to Communicating on the Internet via CityMail, February 4, 1997

New York City Internet Acceptable Use Protocol, 1997

City of New York - Mayor's Office of Operations

Internet Access Guidelines, November 17, 1995.

U.S. Government Publications

A large body of authoritative standards, guidelines and procedures that can assist City agencies in their review and evaluation of information processing environments, and in the development of internal controls and protection plans, are available for City agency use. Federal agencies that publish such data include the National Institute of Standards and Technology (NIST -

an agency of the U.S. Department of Commerce), the Department of Defense (DOD), DOD's Computer Security Center (CSC) and the National Computer Security Center (NCSC).

NIST publishes Federal Information Processing Standards (FIPS PUBS) and other reference materials. These standards and guidelines for data processing system security, interoperability and management are developed for use by Federal agencies, but, in fact, are generic and can be applied to any private or public sector computer system. Some key FIPS PUBS are referenced in the Directive text and listed in Appendix B. A complete listing is available in NIST's Publications List 58, revised as of September 1997. The listing can be accessed on the Internet at http://www.itl.nist.gov/div897/pubs/0-toc.htm. NIST regularly withdraws publications that it considers outdated or better covered by other sources.

A variety of NIST and other publications, their source, and the Internet location where they may be found are identified in Appendix B. Agencies are advised that these publications range from highly specific technical subjects that may be of limited usefulness in managing, protecting and controlling a particular agency's information processing systems, to publications that cover topics that correlate closely with the subject matter of this Directive. Many of the publications contain internal cross references to other materials, suggested reading, and bibliographies.

FEDERAL GOVERNMENT AGENCY PUBLICATIONS

APPENDIX B

Document #	Description	Internet Address (4)
FIPS PUB 105 Federal Information Processing Standards Publication June 6, 1984	Guidelines for Software Documentation Management (1)	See footnote (1)
FIPS PUB 101 June 6, 1983	Guideline for Lifecycle Validation, Verification, and Testing of Computer Software (1)	See footnote (1)
FIPS PUB 106 June 15, 1984	Guidelines on Software Maintenance (1)	See footnote (1)
FIPS PUB 112 May 30, 1985	Password Usage (1)	http://www.itl.nist.gov/fipspubs/fip112.htm
FIPS PUB 113 May 30, 1985	Computer Data Authentication (1)	http://www.itl.nist.gov/fipspubs/fip113.htm
FIPS PUB 127-2 June 2, 1993	Database Language SQL (1)	http://www.itl.nist.gov/fipspubs/fip127-2.htm
FIPS PUB 140.1 January 11, 1994	Security Requirements for Cryptographic Modules (1)	http://csrc.nist.gov/publications/fips/fips1401.htm
FIPS PUB 146.2 May 15, 1995	Profiles for Open Systems Internetworking Technologies (POSIT) (1)	http://www.itl.nist.gov/fipspubs/fip146-2.htm
FIPS PUB 151-2 May 12, 1993	Portable Operating System Interface (POSIX)- System Application Program Interface (C LANGUAGE) (1)	http://www.itl.nist.gov/fipspubs/fip151-2.htm
FIPS PUB 161.2 April 29, 1996	Electronic Data Interchange (1)	http://www.itl.nist.gov/fipspubs/fip161-2.htm
FIPS PUB 179.1 May 15, 1995	Government Network Management Profile (GNMP) (1)	http://www.itl.nist.gov/fipspubs/fip179-1.htm
FIPS PUB 188 September 6, 1994	Standard Security Label for Information Transfer (1)	http://www.itl.nist.gov/fipspubs/fip188.htm
FIPS PUB 46-2 December 30, 1993	Data Encryption Standard (1)	http://www.itl.nist.gov/fipspubs/fip46-2.htm
FIPS PUB 191 November 9, 1994	Guideline For The Analysis of Local Area Network Security (1)	http://www.itl.nist.gov/fipspubs/fip191.htm
FIPS PUB 192 December 7, 1994	Application Profile for The Government Information Locator Service (GILS) (1)	http://www.itl.nist.gov/fipspubs/fip192.htm
FIPS PUB 193 February 3, 1995	SQL Environments (1)	http://www.itl.nist.gov/fipspubs/fip193.htm
FIPS PUB 195 August 15, 1995	Federal Building Grounding & Bonding Requirements for Telecommunication (1)	http://www.itl.nist.gov/fipspubs/fip195.htm
FIPS PUB 196 February 18, 1997	Entity Authentication Using Public Key Cryptography (1)	http://csrc.nist.gov/publications/fips/fips196/fips196.pdf

FEDERAL GOVERNMENT AGENCY PUBLICATIONS

Document #	Description	Internet Address (4)
FIPS PUB 4-1 January 27, 1988	Representation for Calendar Date and Ordinal Date for Information Interchange (1)	http://www.itl.nist.gov/fipspubs/fip4-1.htm
FIPS PUB 87 March 27 1981	Guidelines for ADP Contingency Planning (1)	See footnote (1)
FIPS PUB 95-1 January 4, 1993	Codes for the Identification of Federal and Federally Assisted Organizations	http://www.itl.nist.gov/fipspubs/fip95-1.htm
FIPS PUB 102 September 27, 1983	Guideline for Computer Security Certification and Accreditation (1)	http://csrc.nist.gov/publications/PubsFIPS.html
NIST SP 500-169 National Institute of Standards and Technology December 1, 1989	Executive Guide to the Protection of Information Resources (2)	Publication no longer available on internet.
NIST SP 500-170 December 1, 1989	Management Guide to the Protection of Information Resources (2)	See footnote (2)
NIST SP 500-171 December 1, 1989	Users' Guide to the Protection of Information Resources (2)	See footnote (2)
NIST SP 174 December 3, 1990	Guide for Selecting Automated Risk Analysis Tools (2)	See footnote (2)
NIST SP 500-166 June 6, 1990	Computer Viruses & Related Threats (A Management Guide) (2)	See footnote (2)
NIST SP 800-8 August 13, 1993	Security Issues in the Database Language SQL (2)	See footnote (20
NIST SP 800-12 February 7, 1996	An Introduction to Computer Security: The NIST Handbook (2)	http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf
NCSC-TG-003 National Computer Security Center September 30, 1987	A Guide to Understanding Discretionary Access Control in Trusted Systems (3)	http://csrc.nist.gov/publications/secpubs/rainbow/tg003.txt
NCSC-TG-004 October 21, 1988	Glossary of Computer Security Acronyms (3)	http://csrc.nist.gov/publications/secpubs/rainbow/tg004.txt
NCSC-TG-005 July 31, 1987	Network Interpretation (3)	http://csrc.nist.gov/publications/secpubs/rainbow/tg005.txt
NCSC-TG-006 March 28, 1988	A Guide to Understanding Configuration Management In Trusted Systems (3)	http://csrc.nist.gov/publications/secpubs/rainbow/tg006.txt
NCSC-TG-007 October, 6, 1988	A Guide to Understanding Design Documentation (3)	https://www.fas.org/irp/nsa/rainbow/tg007.htm
NCSC-TG-008 December 15, 1988	A Guide to Understanding Trusted Distribution in Trusted Systems (3)	http://csrc.nist.gov/publications/secpubs/rainbow/tg008.txt
NCSC-TG-009 September 16, 1988	Computer Security Subsystem Interpretation (3)	http://www.fas.org/irp/nsa/rainbow/tg009.htm
NCSC-TG-011 August 1, 1990	Trusted Network Interpretation Environments Guideline (3)	http://www.fas.org/irp/nsa/rainbow/tg011.htm
NCSC-TG-013 June 23, 1989	Rating Maintenance Phase Program (3)	http://www.fas.org/irp/nsa/rainbow/tg013-2.htm

FEDERAL GOVERNMENT AGENCY PUBLICATIONS

Document #	Description	Internet Address (4)
NCSC-TG-014 April 1, 1989	Guidelines for Formal Verification Systems (3)	http://csrc.nist.gov/publications/secpubs/rainbow/tg014.txt
NCSC-TG-015 June 1989	A Guide to Understanding Trusted Facility Management (3)	https://www.fas.org/irp/nsa/rainbow/tg015.htm
NCSC-TG-016 October 1992	Guidelines for Writing Trusted Facility Manuals (3)	https://www.fas.org/irp/nsa/rainbow/tg016.htm
NCSC-TG-017 September 1, 1991	Guide to Understanding Identification & Authentication in Trusted Systems	https://www.fas.org/irp/nsa/rainbow/tg017.htm
NCSC-TG-019 May 2, 1992	Trusted Product Evaluation Questionnaire (3)	http://csrc.nist.gov/publications/secpubs/rainbow/tg019.txt
NCSC-TG-020-A August 18, 1989	Rationale for Selecting Access Control List Features For The Unix System (3)	https://www.fas.org/irp/nsa/rainbow/tg020-a.htm
NCSC-TG-021 April 1991	Trusted Database Management System Interpretation (3)	https://www.fas.org/irp/nsa/rainbow/tg021.htm
NCSC-TG-025 September 1991	A Guide to Understanding Data Remanence in Automated Information Systems (3)	https://www.fas.org/irp/nsa/rainbow/tg025-2.htm
NCSC-TG-026 September 1991	A Guide to Writing the Security Features Users Guide for Trusted Systems (3)	https://www.fas.org/irp/nsa/rainbow/tg026.htm
CSC-STD-002-85 Computer Security Center April 12, 1985	Department of Defense Password Management Guideline (3)	http://csrc.nist.gov/publications/secpubs/rainbow/std002.txt
CSC-STD-003-85 June 25, 1985	Guidance for Applying the Department of Defense Trusted Computer system Evaluation Criteria in Specific Environments (3)	http://csrc.nist.gov/publications/secpubs/rainbow/std003.txt
CSC-STD-004-85 June 25, 1985	Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements (3)	http://csrc.nist.gov/publications/secpubs/rainbow/std004.txt
DOD5200.28-STD Department of Defense December 1985	Department of Defense Trusted Computer System Evaluation Criteria (3)	https://www.fas.org/irp/nsa/rainbow/std001.htm

(1) To obtain a hardcopy, call (703) 605-6585 or write to:
helpdesk@ntis.gov

(2) To obtain a hardcopy, call the GPO at 866.512.1800 or write to:

ContactCenter@gpo.gov

(3) To obtain a hardcopy, call:

NSA Information Security Organization
Service Center at (800) 688-6115 or write to:
www.nsa.gov

(4) Related Internet Addresses. If there is any difficulty accessing the documents at the addresses provided in the table, the following websites may be helpful in providing alternate access information: http://cs-www.ncsl.nist.gov/
http://www.fas.org/irp/nsa/rainbow.htm
http://www.nist.gov/itl/div897/pubs/