Information Resource Security Policies

Proposed by the Security Working Committee (ISS and Clerk of the Court)
Palm Beach County, Florida
Effective October 1, 2000
Information Resource Security Policies

Table of Contents

Information Resource Security Policies

Proposed by the Security Working Committee (ISS and Clerk of the Court)
Palm Beach County, Florida
August 14, 2000

I. Background and Purpose

Complex governmental operations in Palm Beach County rely heavily upon the application of computer-based and shared network systems for their accomplishment. Rapid advances in technology point to increasing dependence of the County governmental entities, constitutional officers, state agencies and the judiciary on shared information and automated systems. The value of such data and software, in terms of restoration costs or losses, far exceeds the value of any associated hardware. Accordingly, information processed by such computerized systems must be protected as a major asset of all the governmental users involved.

The purpose of the Security Policies are to delineate requirements for information security. These requirements are intended to reasonably mitigate the risks that information resources will be destroyed, lost, improperly accessed, incorrectly modified, or not readily available for their intended purposes. Participation in and establishment of a system of controls to offset these threats and protect such shared information resources is a management responsibility of all governmental entities using and contributing to such shared information resources.

The Security Policies will be frequently updated as policies, procedures and practices are added, deleted, or modified. This document will be posted on the Palm Beach County Intranet for ease of access by all interested parties.

II. Definitions:

As used in these Security Policies, unless the context or subject matter otherwise requires:

a. "Confidential Data" means information which is confidential by law or Court Order and therefore requires protection from unauthorized access.

b. "employee" means any employee of Palm Beach County or any Enterprise User.

c. "Enterprise Users" means the Palm Beach County Clerk of the Circuit Court, Board departments and agencies, Court Administrator, Palm Beach County Sheriff, State Attorney, Public Defender, Property Appraiser, Tax Collector, and the Palm Beach County Judiciary insofar as these agencies use the shared IT Facility, including all employees of any of the forgoing.

d. "JIS" means those portions of the IT Facility which are required for processing and storage of Judicial Information System programs for the Civil, Criminal and

Juvenile Courts of Palm Beach County.

e. “ISS” means the Department of Information Systems Services of Palm Beach County and said department’s employees.

f. “IT Facility” means all computers, servers, networks, hardware, software and information resources processed by or residing thereon which are provided by the Board of County Commissioners of Palm Beach County or supported by ISS.

g. “Remote Systems” means computers, devices and hardware which are not supported by ISS, but which have authorized access to the IT Facility, and distributed portions of applications which are part of the IT Facility or JIS but which reside on or within such unsupported computers, devices or hardware.

h. “Security Program” means the rules, regulations and procedures established in these Security Policies and all compatible and duly memorialized regulations established by the management of any of the Enterprise Users.

i “Sensitive Data” means information which is not Confidential Data, but which data has been specifically determined by the management of the user to which said information pertains to be critical to the performance of said user’s mission and functions and to which data, therefore, access rights must be limited, but solely to the extent necessary to protect said information from risk of loss or unauthorized alteration.

j. “user” means any authorized person who or process which accesses the IT Facility via any computer terminal or by any other means.

III. <u>Objectives</u>

The objective of the Security Program is to provide a multi-user network environment for the IT Facility and Remote Systems: which provides: (1) confidentiality; (2) integrity; and (3) availability in a shared environment for all information resources residing within or processed by the IT Facility.

IV. <u>Applicability</u>

Policies contained herein apply to all departments and agencies of the Board of County Commissioners. Approval of these policies by the Justice Information Systems Policy Board binds the Enterprise Users to these requirements insofar as they pertain to JIS. All departments and agencies of County government, including the Constitutional Offices and other Enterprise Users, are encouraged to establish and memorialize compatible security programs and policies which conform with and supplement the requirements set forth in these Security Policies. In the event of any incompatibility between the policies of this Security Program and the supplemental policies of any Enterprise User, the policies in these Security policies shall govern until any such conflicting policies have been harmonized and these Security policies have been formally amended to deal with any such issues.

V. Program

The Security Program will utilize security features resident in the operating and applications programs, as part of an overall plan of security administration and controls, including policies and procedures. The security program is predicated on the analysis and understanding of risk factors used to identify threats to information resources, processing, disclosure, communications, integrity, and availability. These Security Policies deal primarily with the requisite policies and procedures required to establish adequate security (i.e., confidentiality, integrity, and availability) for the information resources of the IT Facility, including, but not limited to, data contributed by or pertaining to any Enterprise User.

VI. Security Exposures:

The following exposures have been identified:

a. Potential Threat Agents:

1. Non-Malicious Users of the System

   such as: users, system operators or administrators, custodians, etc.

2. Other Users of the System

   such as: disgruntled users or corrupt employees.

3. Unauthorized Users of the System

   such as: former users of the system (ex-employees), hackers, or other persons with malicious intent.

4. Inanimate Threat Agents

   such as: water damage (e.g., from leaking pipes), power surges and failures (e.g.,from electrical storms), physical calamities (e.g., from fires, floods, civil unrest), hardware failure within the System, malfunctioning or disabled external devices and systems.

b. Inappropriate Disclosure Threats (Confidentiality Violations)

1. Passive Observation

such as: exposure (e.g., via system malfunctions); inappropriate disposal of used media; eavesdropping (e.g., on video displays); wiretapping or other forms of signal interception.

2. Hardware Attacks

   such as: theft of physical media; physical trespass and observation; implanting eavesdropping devices; disarming controls (e.g., via routine maintenance).

3. Masquerade

   such as: individuals who impersonate (e.g., via password guessing); processes that impersonate (e.g., Trojan horses)

4. Misuse of Authority

   such as: deliberate disclosure; misuse of administrative privilege (e.g, unauthorized modification of access control attributes or editing of password files); exploiting product vulnerabilities (e.g. inadequate authentication, trap doors, improper initialization or recovery, hardware flaws); willful neglect and other errors of omission (e.g., failing to log out when leaving a terminal); preparation for misuse (e.g., code breaking efforts, off-line password guessing, creating, planting and arming malicious software).

c. **Fault-and-Error Threats (Integrity Violations)**

1. Hardware Attacks

   such as: implanting malicious hardware; disarming hardware controls; malfunctioning hardware, etc.

2. Lack of Adequate Competence

   such as: accidental falsification via data entry or modification; installation of flawed software; misapplication of software (e.g., application to wrong data; mis-communication of inputs; improper runtime environment); accidental deletion of critical data.

3. Masquerade

   See section b.3.

4. Misuse of Authority

See section b.4.

d. **Loss-of-Service Threats (Availability Violations)**

1. Inherent System Inadequacies

   such as: inadequate deadlock avoidance; inadequate response to transient errors.

2. Hardware Threats

   such as: deliberate hardware modification (e.g., disabling critical components, shutting off power supply, implanting self destruct devices); inadvertent hardware modification (e.g, normal aging of components, routine maintenance, accidental damage).

3. Usage Threats

   such as: deliberate denial of service or misuse of administrative privileges (e.g., see above); failure to order routine supplies; failure to perform routine maintenance; system shutdown; disabling user accounts; incorrect setting of security attributes; accidental deletion of critical data; system overload.

VII. Security Policies and Procedures

In order to provide security against the threats identified above, it is necessary to implement the security features of the application and operating software in combination with established policies and procedures. The ability of a security program to achieve the desired level of protection against potential security risks depends jointly on the correctness of the mechanisms within the IT Facility itself, the protection of those mechanisms to ensure their correctness, and on adherence to associated usage security policies by authorized users. In combination with the operating and application software acquired, it is the object of this Security Program to establish policies and procedures which provide for: (1) accountability; (2) access control; (3) availability; and (4) security management, consistent with the assumed threat environment based upon ongoing risk analysis.

The ability to successfully achieve these purposes jointly depends upon (1) the consistency of the security features of the hardware and software being used with the Security Program objectives; (2) the correct operation and input by IT Facility administrative personnel (e.g., IT Facility start-up or recovery must be performed properly; the user registration and the IT Facility entry parameters must be set properly); and (3) the actions of the users themselves (e.g., choice of passwords, setting of default access rights, distribution of access rights, competence, etc.).

a. **Accountability**

1. The policies and procedures provide mechanisms to support the accountability functions contained in the operating and application software. The IT Facility software assigns responsibility for an action to an accountable entity (i.e., the identified and authenticated individual whose security policy attributes may include name, role, group, and/or security level).

2. The following functional components exist:

   a. Identification and authentication components which establish the authenticity of the claimed identity by the user.

   b. IT Facility entry components which provide the appropriate time, location, and mode-of-entry context for each user's interactions.

   c. Trusted path components which ensure that nothing can interfere with the interactions between the IT Facility and the authenticated user.

   d. Audit components which ensure that user interactions are recorded and attributed to the accountable user identity.

b. **Access Control**

The policies and procedures provide mechanisms to support the access control functions contained in the operating and application software. The objectives of the access control policies relate primarily to the confidentiality (prevention of unauthorized disclosure) and data integrity (prevention of unauthorized modification or destruction of data) aspects of IT Facility security. Via the development and maintenance of an Access Control List (which constitutes a list of all authorized users who are authorized to have access to any resources of the IT Facility) the Security Program will ensure that system information is disclosed only to authorized persons and will prevent the unauthorized modification or destruction of IT Facility data. The Enterprise Users themselves will be responsible for defining the access privileges of each of their employee-users, as well as access rights related to other users who belong to groups of users which may properly have access to Confidential Data or Sensitive Data. Additionally, the security policies provide for limitation of administrative access, and accountability - via the audit function - for the purposes of administration and maintenance of the IT Facility. With respect to administrative (ISS) access to Confidential Data, the policies provide for desensitizing such data if it must be viewed or otherwise accessed by humans for testing or maintenance purposes, and assuring the trustworthiness of employees by performing criminal background checks on those granted administrative access.

c. **Availability Policy (for Justice Information Systems)**

The operating and application software for JIS will be designed for a High Availability environment, will be fault tolerant and, if required, will have the ability to be configured to allow prioritization of IT Facility resources.

d. **Security Management**

1. The security management functions are required to counter the same risks as those countered by the security policy functions listed above (i.e., accountability, access control, and availability). This is the case because the security management functions implement a significant part of all the Security Program. In addition, the security management functions have been partitioned into different administrative roles, to help limit any potential damage caused by unskilled or malevolent administrators.

2. Security policies will address:

   Definition and update of user security characteristics (e.g., unique identifiers associated with user names, user accounts, per-user policy attributes, system entry parameters, availability parameters or resource quotas).

   Definition and update of security policy parameters (e.g., identification and authentication, system entry, access control, communications protocols and availability parameters).

   Routine control and maintenance of IT Facility resources (e.g., enable and disable peripheral devices, handling and disposal of removable storage media, backup and recovery of user objects, and routine maintenance of IT Facility hardware and software elements).

   Auditing both privileged and unprivileged user actions, and audit management (e.g., selection of audit events, management of audit trails, audit trail analysis, and audit report generation).

3. Additional security policies will be developed in the future to address IT Facility generation, installation, configuration, and non-routine maintenance (e.g., IT Facility manual recovery, installation of "patches," correcting security flaws, repair of damaged IT Facility hardware and software elements).

VIII. <u>Consequences of Policy Violations</u>

Employees violating this policy are subject to disciplinary action, including possible termination. Severity of the disciplinary action and/or legal action will depend upon the nature of the offense and will be governed by the County’s Merit Rules and User Department/Agency procedures.

Deleting and/or altering official records constitutes a third degree felony as Official Misconduct per Florida Statutes 839.25 and a first degree misdemeanor as Falsifying Official Records per Florida Statute 839.13.

1.0 Security Program Organization

1.1 Purpose:

This policy sets forth the duties and responsibilities of the Department of Information Systems Services (ISS) with regard to the administration of a centralized security program for the information resources resident in the IT Facility.

1.2 Policy Overview:

A centralized security program is established to administer the overall policies and procedures applicable to system security. ISS is the designated agency responsible for staffing and coordinating the centralized security administration functions.

Effective security involves many elements of the organization and multiple layers of the technical infrastructure. The Security Program involves the broad aspects of computer controls, including: system access; physical security; IT Facility software; application development and change controls; segregation of duties; service continuity; and effectiveness monitoring and evaluation of security procedures.

1.3 Policy Provisions:

Security risks are applicable to both the traditional mainframe-based systems and distributed, client server systems. ISS will administer a formal**,** centralized security program with the intent of meeting the following objectives:

a. assure that an adequate computer security planning and management program is in place;

b. protect data, files, and programs from unauthorized access, modification, or destruction;

c. limit and monitor access to programs and files that control computer hardware and secure applications;

d. prevent the introduction of unauthorized changes to systems, applications software, or data;

e. prevent any single individual from controlling key aspects of computer-related operations; and

f. ensure the recovery of computer processing operations in the event of a disaster or other unexpected disruption.

ISS will maintain a full-time Security Administrator who will be responsible for supervising and coordinating the day-to-day activities of the security function. To assure independence within the ISS Department, this position will report~~s~~ directly to the Department Director.

County Departments and Enterprise Users will mutually cooperate and provide the management resources necessary to ensure that: (a) this Security Program for the IT Facility is fully developed: (b) the Security Policies will be jointly and periodically reviewed; and (c) full cooperation is extended to ISS in the administration of the security function for the IT Facility and to the Enterprise Users in connection with Remote Systems under their control

The Security Administrator will be responsible for developing and maintaining security-related policies and procedures applicable to the IT Facility. This will require communication and coordination with all departments and agencies using shared and stand-alone information systems. The Security Administrator will provide the direction and technical expertise to ensure that the IT Facility and its information resources are properly protected. This includes consideration of the confidentiality, integrity, and availability of both information and the systems that handle it, as well as the resources available to address these issues.

The Security Administrator will act as a liaison on information security matters between all County agencies, departments and divisions, and will serve as the focal point for all information security activities for Enterprise Users. The Security Office must perform risk assessments, prepare action plans, evaluate vendor products, participate on in-house development projects, assist with control implementations, investigate information breaches, and perform other activities which are necessary to assure a secure information handling environment.

The Security Administrator will distribute and make available (in print and electronic format) copies of the PBC Enterprise Security document which contain the detailed security policies and procedures.

1.4 Audit Reviews of Information System Controls

The Internal Audit Department will periodically review the adequacy of information system controls as well as compliance with such controls. The Security Administrator will serve as the ISS liaison in matters relating to the audit.

The County’s external auditors may also evaluate the adequacy of security controls as part of their audit of the financial records. Any assistance required by the auditors will be coordinated by the Security Administrator.

2.0 Personnel Security

2.1 Purpose:

The purpose of this policy is to delineate requirements for employee conduct and personnel administration in matters relating to security.

2.2 Policy Overview:

The human element is the most important component of any security program. Knowledgeable and trustworthy users are essential in ensuring that adequate controls exist and are complied with. This policy addresses security-related matters involving the hiring, training, discipline, and termination of users.

2.3 General Policy:

2.31 Avoidance of Actual and Apparent Conflicts of Interest

a. All users must avoid actual or apparent conflicts of interest in their dealings with companies or individuals doing business with Palm Beach County. Should there be any doubt as to the existence of a potential conflict of interest, the user must consult his or her manager. If necessary, an opinion should be sought from the County Attorney's Office.

2.32 Disciplinary Measures for Non-Compliance with Information Security Policies

a. Non-compliance with information security policies, standards, or procedures is grounds for disciplinary actions up to and including termination.

- Assuming the non-compliant act is inadvertent or accidental, first violations of information security policies or procedures must result in a warning. Second violations involving the same matter must result in a letter being placed in the involved user's personnel file and a five-day suspension without pay. Third violations involving the same violation must result in dismissal. Willful or intentional violations, regardless of the number of violations, may result in disciplinary action up to and including immediate dismissal.

2.33 Handling Involuntary Terminations of System Users

a. In all cases where information technology users are involuntarily terminated from employment, they must be immediately relieved of all of their duties, required to return all Palm Beach County or Enterprise User equipment and information, and escorted while they pack their personal belongings and leave the facilities.

2.34 Actions to be Taken in Response to Terminations of Employees or Contractors

a. In the event that an employee, consultant, or contractor is terminating his or her relationship with Palm Beach County or an Enterprise User, or is being involuntarily terminated, the worker's immediate manager is responsible for (1) ensuring all property in the custody of the user is returned before the worker leaves the County premises; (2) notifying all administrators handling the computer and communications accounts used by the users as soon as the termination is known, and (3) terminating all other work-related privileges of the worker at the time that the termination takes place.

2.35 Notification of Outside Employment

a. Employees are permitted to have second jobs only under certain circumstances. A second job is not permissible if it may in any way jeopardize or compromise an employee's objectivity when performing duties on behalf of Palm Beach County or any Enterprise User.

b. Second jobs must be disclosed during a prospective employee's initial interview, or when taken if the worker is currently a County employee or employee of an Enterprise User.

2.36 Duty to Report Status Changes Affecting Eligibility for Certain Positions

a. Employees have a duty to promptly report to their immediate manager all changes in their personal status which might affect their eligibility to maintain their current position. If employees fail to disclose material information about their changed status, they subject themselves to disciplinary action up to and including termination. Examples of such status changes include being arrested, charged, advised of the disposition of, or convicted for felony crimes and outside business activities.

2.37 Background Checks for Computer-Related Positions of Trust

a. **Computerized systems must provide reasonable controls to assure**

that data integrity is protected from malicious acts by those personnel responsible for providing technical support and administration of these systems. All workers to be placed in computer-related positions of trust involving the IT Facility must be subjected to a background check. **“Trust” positions for the purpose of this policy are defined as database administrators, UNIX server administrators, and application programmers.** This process shall include examination of criminal conviction records, credit bureau records, driver’s license records, as well as verification of previous employment. This policy applies to new employees, re-hired employees, transferred employees, as well as third parties, e.g., temporaries and existing, contractors, and consultants.

2.38 Information Security Training Required for all Computer Workers

a. All workers (employees, consultants, contractors, temporaries, etc.) must be provided with sufficient training and supporting reference materials to allow them to properly protect Palm Beach County information resources and the resources of the IT Facility.

b. All employees and agents of the County and the Enterprise Users must understand the security policies and procedures for information security for the IT Facility and its data, and must agree in writing to perform their work according to such policies and procedures.

3.0 Acceptable Use of Information Technology Resources

3.1 Purpose:

The following document establishes policies for the use of the computing systems and facilities located at or operated by the Palm Beach County Department of Information Systems Services (ISS), the IT Facility. The purpose of this policy is to ensure that all system users use the IT Facility in an effective, efficient, ethical and lawful manner.

3.2 Policy Overview:

The definition of the IT Facility includes all computers, servers, networks, hardware, software and information resources processed by or residing thereon which are provided by the Board of County Commissioners of Palm Beach County or supported by ISS. Use of the IT Facility includes the use of data or programs stored on ISS enterprise systems, data or programs stored on magnetic tapes, disks, CD ROMs or other storage media maintained by ISS. A "user" is any person who or process which accesses the IT Facility via any computer terminal or by any other means; this includes, but is not limited to, employees and Remote Systems of Enterprise Users.

3.3 Policy Provisions:

The IT Facility is to be used only for the purposes for which it is authorized and is not to be used for non-work related activities. Unauthorized use of information technology resources is in violation of Section 799, Title 18, U.S. Code, and constitutes theft and is punishable by law. Therefore, unauthorized use of IT Facility computing systems and facilities may constitute grounds for either civil or criminal prosecution. In the text below, "users" refers to users of the IT Facility.

a. Classified data (i.e., information that is Sensitive Data or Confidential Data) will be maintained in a secure server environment. Users are responsible for protecting any information used and/or stored on/in Remote Systems managed by departments, agencies or Enterprise Users. The various security-related Policy and Procedure Memoranda (PPMs) should be consulted for policy guidelines on protecting information technology systems and data.

b. Users are to report any apparent security weaknesses or exposures in the IT Facility or any incidents of possible misuse or violation of this agreement, to the proper authorities by contacting the ISS Security Manager or by sending electronic mail to security@co.palm-beach.fl.us.

c. Users shall not attempt to access any data or programs contained in or on the IT Facility for which they do not have authorization or explicit consent of the user or Enterprise User for which said program is intended or whose data resides therein.

d. Users shall not divulge Dial-up or Dial-back modem phone numbers to other persons.

e. Users shall not make unauthorized copies of copyrighted software except as permitted by law or by the owner of the copyright.

f. Users shall not make copies of system configuration files (e.g. password files/etc.) for unauthorized personal use or to provide to other people/users for unauthorized uses.

g. Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of systems; deprive an authorized user access to an information technology resource; obtain extra resources beyond those allocated; circumvent ISS security measures or gain access to the IT Facility or any other Palm Beach County information technology system for which authorization has not been given.

h. Electronic communication facilities (such as e-mail or Internet transmissions) are for authorized government use only, except to the extent that limited personal use is permitted under PPM# CW-R-008. Fraudulent, harassing or obscene messages and/or materials shall not be sent from, to, or stored on the IT Facility.

i. Unauthorized users (individuals not specifically designated through job function, scope of work or special assignment to perform such and activity) or technical staff shall not download, install or run security programs or utilities which reveal weaknesses in the security of a system. For example, Palm Beach County users shall not run password cracking programs on the IT Facility.

Any noncompliance with these requirements will constitute a security violation and will be reported to the ISS Security Manager and the appropriate management personnel of the violator’s assigned department, agency or Enterprise User. Substantiated violations may result in short-term or permanent loss of access to computing systems maintained by ISS. Serious violations may result in civil or criminal prosecution.

As indicated by my signature below, I understand the foregoing policies for acceptable use of information technology systems maintained by ISS, and agree to abide by these requirements.

Signature: _______________________________________ Date: _______________

4.0 Security Training

4.1 **Purpose:**

The intent of this policy is to establish requirements that computer users, technicians and administrators receive training on basic security principles and practices. The content of the training courses will be tailored based on the nature of the employee's role in using or administering the various County-owned computer systems and/or the IT Facility.

4.2 **Applicability**:

This policy applies to all employees, including contract workers, consultants, and all others accessing and using any computer system or network operated or administered by Palm Beach County, including the IT Facility.

4.3 **Policy Overview:**

All workers (employees, consultants, contractors, temporaries, etc.) must be provided with sufficient training and supporting reference materials to allow them to properly protect the County's information resources. Specific training and materials to be provided will vary based on the nature of the worker's job.

4.4 **Policy Provisions:**

4.41 Information Systems Services (ISS) Responsible for Security Training

a. ISS shall provide introductory and refresher courses (and related materials) to educate and regularly remind users about their obligations with respect to information security.

4.42 Information Security Training Required

a. Management must allow sufficient on-the-job time for employees to acquaint themselves with the Security Program, procedures, and related ways of doing business. The training course shall address security risks and exposures, and the counter measures that have been put in place to control these risks.

b. Every worker must understand the policies and procedures of the Security Program about information security, and must agree in writing to perform his or her work according to such policies and procedures.

c. Every employee must attend an information security awareness class within three months of the date when they began employment with Palm Beach County or any Enterprise User. To verify attendance at said course, each attending employee will receive a certificate of course attendance.

4.43 Required User Training for Production Systems

a. Employees or contractors must not use any software, hardware and networks for production business processes unless they have first completed approved training for such systems. Certain critical applications will require additional application specific information security policies. These more detailed policies and procedures shall conform to the general principles set forth in the Information Security Policies.

4.44 Required Training for Personnel Assigned as Security or System Administrators

a. Administrative personnel working in security programs or as system administrators must be trained in all aspects of the security features and functions particular to the information systems which they are assigned. Certain computing environments, such as Internet electronic commerce, may likewise warrant more detailed training for technical support staff.

5.0 Enterprise Center (Computer Room) Access

5.1 **Purpose:**

To establish computer security policies governing physical access to the Enterprise Center (Computer Room) which houses the County's primary computing resources and associated information assets. Additionally, this policy outlines requirements for environmental controls to protect the equipment and systems residing in the Enterprise Center. The data and equipment residing in this area represent information resources of the County, Constitutional Offices and the State, and must be protected to ensure system integrity, dependability and availability.

5.2 **Policy:**

It is the policy of Palm Beach County ISS that the Enterprise Center be accessible only by authorized personnel who require entrance in order to perform their job functions. All others, including those requiring periodic access to perform repairs, resolve problems, or otherwise conduct business with ISS personnel will be admitted on a "request and sign-in" basis for each entry.

5.3 **Responsibility:**

The responsibility for approving badge reader access to the Enterprise Center Computer room is vested with the Enterprise Center Services Manager or the Director of Technical Services. Responsibility for enforcing this policy resides with the Enterprise Center Services Manager and shift supervisors. Violations are to be documented and reported to the ISS Director, Technical Services Director and/or the Security Manager who will determine appropriate actions.

Responsibility for maintaining badge reader access is assigned to the Coordinator who maintains the badge system for ISS. Requests to add or delete access for employees or contractors will be communicated using the "Employee Access Procedure" and form. Requests to temporarily or permanently modify access will be forwarded to the Enterprise Center Services Manager or Technical Services Division Director.

5.4 **Procedure:**

Personnel assigned to work in the Enterprise Center will have badge reader access to the Enterprise Center. The Enterprise Center Manager or authorized person (see Administration of Rights policy) will prepare the "Employee Access Form" for new employees, contractors or staff whose responsibility within the organization has changed (i.e., transfer, termination, etc.).

All other ISS personnel who require periodic access to the Computer Room may request badge reader access from the Enterprise Center Manager or Director of Technical Services. Requests for temporary access will be approved or denied based on the need to limit Enterprise Center access, provide a high level of security, and isolate the production area from unnecessary interruptions.

Visitors are classified into five categories as follows:

5.41 Permanently Assigned Contractors:

a. will receive an access card from the appropriate responsible manager through an "Employee Access Form;" and

b. need not be escorted in their authorized work zones**.**

5.42 Temporarily Assigned Contractors:

a. will sign in and out with the Enterprise Center Shift Supervisor and display a "write-on" sticker during their stay;

b. need not to be escorted in their authorized work zones;

c. must be escorted in all other restricted areas; and

d. will sign out and return sticker when leaving the premises.

5.43 Electricians, Service Personnel:

a. equipment maintenance must be scheduled in advance with the Enterprise Center Manager, preferably at nights, on weekends, or during "non-production" hours;

b. will sign in with the Enterprise Center Shift Supervisor and be given an identification badge to wear for the duration of the visit.

c. need not be escorted in authorized work zone, but will require an escort in all other restricted areas.

d. will sign-out and remove badge when leaving the premises.

5.44 Property Appraiser's Staff and Guests:

a. only authorized access card holder**s** are permitted access to the Property Appraiser's area of the computer room;

b. all others must sign in and out with the Enterprise Center Shift Supervisor; and

c. Authorized Property Appraiser staff must be escorted in all other restricted areas of the computer room.

5.45 Other Visitors:

a. visitors who have arranged for appointments with ISS personnel will receive “write on” stickers, which are valid only for their appointment period, containing the following information: Visitor Name; Visiting Person/Area; and Date/Time.

b. will be escorted throughout their stay by the ISS contact person.

c. will sign out and return sticker when leaving the premises.

A list of names should be provided for large groups visiting the Enterprise Center (e.g., classes, tours, etc.). Individuals who do not work in the Computer Room may gain access to participate in a presentation or for a specific function or Data Center Tour, by calling the Enterprise Center Manager or Shift Supervisor who coordinate the sign-in procedure and provide access.

The Enterprise Center Manager and Shift Supervisors have responsibility for approval/denial to the Computer Room for all personnel who do not have badge reader access. Approval is to be indicated by the ISS Supervisor’s signature on visitor log which will be maintained by the Enterprise Center Shift Supervisor with copies kept on file by the Security Manager.

6.0 System Access Control

6.1 Purpose:

To establish policies governing the management and maintenance of User Identification (IDs) names, numbers and passwords for the IT Facility. This policy outlines requirements to protect the hardware, software and information resources of the County, Constitutional Offices, Enterprise Users and the State to ensure system integrity, dependability and availability.

6.2 Policy Overview:

System access is critical to County agencies, Enterprise Users, and members of the public who seek to obtain information under the provisions of the Florida Statutes. Any government organization must have access to information required in the performance of its duties. Governmental organizations also provide open access to public records, but unrestricted access to public records has the potential to adversely affect, rather than enhance, organizational service objectives. This policy provides for secured access to data systems using User ID and password standards and requirements.

6.3 Policy Provisions:

This policy applies to all employees using or persons accessing computers systems and programs constituting part of the IT Facility, from any location during working and non-working hours. All such persons are referred to hereinafter as “users.” This policy also applies to contractors and volunteers who are authorized to access the IT Facility. All such workers, employees and contractors, who access County data systems will be required to enter a User ID and password before gaining system access.

6.31 User IDs shall meet the following standards:

a. User IDs must not exceed eight (8) characters;

b. User IDs will be composed of the first character of the user’s first name followed by up to seven characters of the user’s last name;

c. In cases where employees have the same first and last name, the User ID will incorporate the user’s middle initial. A user’s middle initial will follow the first character of the User ID; and

d. User IDs will be consistent across all systems whenever possible.

6.32 Passwords will meet the following standards:

a. passwords must contain a minimum five (5) characters;

b. passwords will not be reused.; and

c. all user-chosen passwords for computers and networks must not be shared, divulged to others, or obviously attributable to the user (i.e., J. Baker = baker1).

6.33 Compliance Requirements (Based on System Software Capabilities)

a. Compliance with User ID and password standards will be checked at the time the users construct or select them. User IDs and passwords will be initially selected by the System Administrator.

b. The number of consecutive unsuccessful login attempts will be limited. After three (3) unsuccessful login attempts, the User ID privileges will be suspended until reset by a Security Administrator or for a time period not less than four (4) hours.

c. Prior to password expiration the user will be notified by the system that the password must be changed.

d. Password changes will be forced by the system after the grace login period, after password changes by the security administrator, and upon initial activation of a new User ID.

6.34 User Responsibilities

a. A user is responsible for all activities performed with his or her personal User ID.

b. User IDs are not to be used by anyone other than the individuals to whom they have been issued.

c. Users will not share passwords.

d. Passwords must not be written down and left in a place where unauthorized persons can discover them.

e. The initial password issued by the Security Administrator must be changed immediately upon entering the system.

f. Users are prohibited from constructing fixed passwords by combining a set of characters that do not change, with a set of characters that change predictably.

g. Passwords must be changed at least every ninety (90) days.

h. In the event of an expired, misplaced or forgotten User ID or password, the affected user must contact the Security Administrator or designee (Customer’s Systems Administrator) to reinstate user access.

i. All requests for the validation of a new User ID must be submitted in writing prior to required activation.

j. Any request for user access modification must be submitted in writing by the appropriate authority.

6.35 Security Administrator Responsibilities

a. Security Administrators will ensure that User IDs and passwords are created and issued upon appropriate request and approval.

b. Requests for additions or modification will be documented in writing.

c. Security Administrators will ensure that a user’s access is removed upon written request by the user’s supervisor.

d. Security Administrators will maintain confidentiality of users.

e. Security Administrators will only disclose User IDs and passwords when a new user ID is being assigned, the affected user is able to provide proof of identity, or the affected user’s supervisor provides a written request.

Passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions that the other party takes with the disclosed password. All passwords must be immediately changed if they are suspected of being disclosed, or known to have been disclosed to anyone besides the authorized user.

Wherever systems software permits, the display and printing of passwords must be masked, suppressed, or otherwise obscured such that unauthorized parties will not be able to observe or subsequently recover them.

All default system passwords must be changed before any computer or communications system is used for business. This policy applies to passwords associated with end-user User-IDs, as well as passwords associated with network, systems administrator and other privileged User-IDs.

To prevent password guessing attacks, where systems software permits, the number of consecutive attempts to enter an incorrect password must be strictly limited. After three (3) unsuccessful attempts to enter a password, the involved User-ID must be either suspended until reset by a System Administrator, or temporarily disabled for four (4) hours. If dial-up or other external network connections are involved, the session must be disconnected.

If the Security Administrator suspects system security has been compromised, reasonable steps should be taken to restrict system access, as appropriate, until the nature of the security threat is determined and addressed. In some cases, this might require that the responsible System reassign all relevant passwords and force every password on the involved system to be changed at the time of the next log-in. If the system software does not provide the latter capability, a broadcast message should be sent to all users instructing them to change their passwords.

Whenever system security has been compromised, or if reasonable suspicion exists, the involved system(s) must be evaluated for suspected system and access modifications. This information might be available through software utilities or review of transaction logs. Similarly, all changes to user privileges taking effect since the time of suspected security violation(s) must be immediately reviewed by the Systems Administrator for unauthorized modifications.

7.0 Access Privileges

7.1 Purpose:

The purpose of this policy is to provide for the establishment and administration of access privileges for users of the IT Facility and any Remote Systems.

7.2 Policy Overview:

Palm Beach County Information Services Department (ISS) is responsible for providing computer services via shared computer systems and networks (“IT Facility”) to multiple user entities, including the County itself and the Enterprise Users. This service includes responsibility for administration and control of security policies and procedures designed to protect the confidentiality, integrity, and availability of the user data residing in said IT Facility. Each of the multiple user entities and Enterprise Users supplying data to the IT Facility is responsible for establishing and defining, in technical cooperation with ISS, the access privileges to be granted to any user other than ISS to the extent that such privileges permit any user to access the production data of said entity residing within the IT Facility.

With respect to distributed programs residing on the IT Facility, each user entity or Enterprise User is itself responsible for implementing and administering any access security features for its own Remote Systems or its own employee-users, when such access security features reside in the Enterprise User’s Remote System and where ISS has elected to configure and enable such access security features to be implemented and administered by said Enterprise User as part of this Security Program. All such administration of the security features of Remote Systems or distributed applications shall be compatible with the overall intent of this Security Program and in the event of any conflict, all such conflicting policies or administrative actions shall be immediately amended and harmonized, consistent with a centralized Security Program for a shared network environment. ISS, in cooperation with the respective user entities or Enterprise Users, shall be responsible for establishing and defining access privileges for users within ISS or outside vendors for the sole purposes of operation and maintenance of application programs and the operating, communication, and systems applications for the IT Facility, consistent with the defined security needs and requirements of the respective user or Enterprise User entities.

7.3 Policy Provisions:

7.31 User Responsibilities

a. The System Administrator representing each entity or Enterprise User using the IT Facility shall be responsible to provide ISS with a separate written user profile (for each employee-user) defining the specific access privileges of each employee of said user entity or Enterprise User who is to have access to its production data or portions thereof residing within the IT Facility. The privileges to be defined and specified include: create; read; write; delete; update, etc. Additionally, said information shall specify which production data within their specified database should not be accessible to said user-employee and the reason (e.g., exempt information under public records act, court order, adoption records, juvenile records, proprietary information, etc.).

b. Confidential Data means information which is confidential by law; i.e., information which requires protection from unauthorized access by virtue of its legal exemption from the Public Records Act, Court order or other legal reason. Each entity or Enterprise User supplying Confidential Data to the IT Facility shall be responsible to provide ISS with written information concerning which classes of data, data tables or segments of any informational database within the IT Facility should be treated as Confidential Data. With respect to such Confidential Data, each user entity or Enterprise User supplying such data shall also advise ISS regarding which other users or user entities, as the case may be, are authorized to have limited or other access to said Confidential Data. Each entity user or Enterprise user shall be responsible for providing ISS with a separate written user profile, as provided in paragraph 7.31a. above, and beyond a separate writing as provided above, with respect to any vendor or other non-employee authorized by said user entity to have access to its production data, Sensitive Data or its Confidential Data residing in the IT Facility.

c. To the extent that shared and distributed applications within the IT Facility permit and are so configured and distributed by ISS to enable user entities or Enterprise Users to establish user access privileges at the user level, each such user entity shall be solely responsible for the establishment, implementation and maintenance of security access privileges within said application for its own employee-users.

7.32 ISS Responsibilities

a. ISS shall take all necessary and reasonable measures to ensure that the access privileges defined in the written user profiles supplied by all user entities and Enterprise Users are effectively and efficiently implemented at all appropriate levels of the application and operating system programs, except that the entity users and Enterprise Users shall be responsible for said implementation at the application program levels, where security features of such applications are configured to be and have been distributed to them by ISS.

b. ISS shall take all necessary and reasonable measures to ensure that Confidential Data residing in the IT Facility is accessible only in accordance with access privileges as defined in the written information provided by the user entity or Enterprise User which initially supplied such Confidential Data. ISS shall further take all necessary and reasonable measures to ensure that access to such Confidential Data is confined and restricted, as specified, at all appropriate levels of the application and operating system programs, except that the entity users or Enterprise User shall be responsible for said implementation at the application program levels, where security features of such applications are so configured and distributed to them by ISS.

c. ISS shall establish access privileges for ISS personnel or outside vendors which limit the privileges of said users to only such access as is required for them to perform the maintenance and operational functions to which they are assigned.

d. In connection with required maintenance and operation activities by ISS and authorized outside vendors requiring access to the production data or Confidential Data of user entities, ISS shall:

- restrict the number of ISS personnel authorized to conduct said activity to the minimum number required to perform such activities and require that these persons have a high level of security clearance; and

- require that an audit report be generated with respect to any access, other than by automated processes, to said production data or Confidential Data; and

- take all such other measures as may reasonably be required to prevent the unauthorized disclosure or use of any such production data or Confidential Data, including sufficient desensitization of any Confidential Data in coordination and cooperation with the user entity or Enterprise User supplying said data, prior to the actual viewing of any such data by ISS or vendor personnel. As used herein, the term “sufficient” means that enough elements of the Confidential Data are obscured or unavailable for human viewing such that the remainder of the available data is without contextual significance and, therefore, does not reveal meaningful information.

8.0 Maintaining Security Profiles

8.1 **Purpose:**

To provided policy guidelines for determining the roles that ISS and the users of the IT Facility, including Enterprise Users, will assume in maintaining the security within an application.

8.2 **Policy Overview**:

Palm Beach County Information Systems Services (ISS) provides automated systems and data storage for various Enterprise Users of the County's IT Facility. As such ISS is primarily responsible for the implementation of a jointly established Security Program which is adhered to by all users and Enterprise Users in order to best provide for confidentiality, integrity and availability of data and information resources supplied to such IT Facility by said users. Management of the Enterprise Users has the responsibility to cooperatively participate in the establishment and oversight of a joint Security Program which will enable the IT Facility to provide a secure environment for data and information resources which are input, contributed to, or shared within the IT Facility. ISS has primary responsibility to maintain the IT Facility and implement the joint Security Program therefore.

Computer systems require regular review and updating of their security programs. Maintenance and review of the Security Program must be done in a timely and cost efficient manner to ensure achievement of the Security Program goals of confidentiality, integrity and availability of IT Facility data. Consequently, it is important that all of the Enterprise Users participate in an ongoing and cooperative manner, and with qualified technical personnel, in ongoing issues relating to the Security Program and security policies arising out of reprogramming because of problems found or enhancements requested by users or Enterprise Users.

Many newer applications enable an end-user of a distributed application to self administrate various aspects of the application. Newer applications can also provide features which permit the establishment of profiles for groups of similarly privileged users for purposes of program access within a shared environment allow techniques that can lower the time involved with maintaining user profiles and program access or other features. One technique used is the grouping of like individuals or programs into a class or group. When grouping is utilized, it allows the security administrator to make one change that can affect many users within a group instead of having to make the same change many times for each individual member.

This policy is intended to define the responsibilities of Enterprise Users and Security Administrators of systems to ensure that security and program maintenance is performed in a timely, cost efficient and correct manner.

8.3 **Policy Provisions:**

Each user and Enterprise User must define to ISS the access rights of its employees (i.e., the different classes of its users). These classes may exist because of function, organizational structure, Confidential Data, or other business reasons. With respect to ISS, each Enterprise User or other user who is legally responsible for the protection of Confidential Data contributed to or residing within the IT Facility, must identify such data to ISS in the manner described in Section 7.0 of these Security Policies and the appropriate security measures and restriction of access must then be invoked.

In applications that allow distributed rights to define and maintain the groups, classes, or profiles within that application, the Enterprise User to which said rights are distributed, if any, shall have primary responsibility for defining and maintaining the groups, classes, or profiles within that application applicable to that Enterprise User's employee-users. However, the establishment of groups, classes, profiles, etc., shall follow the format established for the application. In the event that there are conflicts between various Enterprise Users concerning the access rights of any of its employee-users to JIS information resources within the IT Facility, such conflicts shall be immediately reported to ISS which shall present the issues to the Chief Judge of the 15th Judicial Circuit for resolution. Upon such resolution, any such access rights shall be forthwith established or modified in accordance with the written directive of the Chief Judge.

Any changes in distributed security functions (including, but not limited to, the maintenance of user-groups, classes or profiles) made by Enterprise Users or security administrators for Remote Systems shall be documented and reported to ISS for updating of its Master Access Control List and said Enterprise User or Security Administrator documentation shall be maintained as long as that change remains within the Remote System.

9.0 Classification of Data for Restricted Access

9.1 Purpose:

To provide policy guidelines for classifying data that requires restricted access.

9.2 Policy Overview:

Palm Beach County Information Systems Services (ISS) provides data storage for Palm Beach County and various Enterprise Users of the IT Facility. As such, ISS has responsibility for the implementation of a joint Security Program to protect such data. Each user of the IT Facility is in the best position to determine the level of access to the data it contributes to the IT Facility that groups or classes of individual users need, as well as the rights of the public to view such information. When contributed data is Sensitive Data or Confidential Data, it is the responsibility of the Enterprise User contributing such data to identify and establish restrictions for accessing said data, consistent with the law and the overall objectives of the Security Program.

9.3 Policy Provisions:

Each Enterprise User or other contributors of data to the IT Facility is responsible for determining the sensitivity of data it has contributed or for which it is legally responsible. This determination can come from statutes, policy, guidelines, or generally accepted practices. Once data is determined to be Sensitive Data, or Confidential Data, its degree or levels of sensitivity must also be established in writing by the Enterprise User who is responsible for said data. Additionally, each Enterprise User or other contributor of data is responsible for taking into account the various legal requirements for public access to judicial and governmental records as contained in Rule 2.051, Judicial Administration Rules, and section 119.07, Florida Statutes, among others. Access restrictions requested by Enterprise Users must be consistent with the right of public access for viewing such information and requested classifications and restrictions should be limited to those categories and measures which are sufficient to protect the integrity or prevent the loss of Sensitive Data and guard against the unauthorized disclosure of Confidential Data, while otherwise permitting lawful viewing of data to which the public is entitled to access. Erroneous classification or restriction of viewing access will be the responsibility of the Enterprise User that requested such classification or restriction. It is the responsibility of ISS only to know and maintain the different levels of data sensitivity as reported to it by the respective Enterprise Users.

10.0 Database Security

10.1 Purpose:

To establish policy for access to databases maintained by the Information Systems Services Department and to define the appropriate levels of security auditing for databases used by County agencies or Enterprise Users.

10.2 Policy Overview:

This policy establishes standards for auditing production databases to assure the security of data maintained within these systems. These standards will require that roles be assigned to users and ISS personnel commensurate with the access required to perform job-related tasks. User name and password requirements are addressed in another section of the Security Policies.

To minimize the impact of auditing on the performance of a production system, and control the size of the audit trail, each system should be independently evaluated. This analysis will aid in devising the proper auditing strategy for that system and avoid unnecessary processing overhead.

10.3 Policy Provisions:

This policy applies to all databases residing on the IT Facility. This policy also applies to contractors and volunteers who are authorized to use the IT Facility.

It is the general policy that database services are to be audited at a sufficient level to ensure responsible, ethical, and legal access and manipulation of IT Facility data. Willful or intentional misuse, alteration, destruction or corruption of such data will result in disciplinary action under applicable provisions of the Palm Beach County Merit Rules, as well as possible criminal charges.

10.31 Audit Levels

a. Development, test, training and quality assurance databases will not normally be audited. The default will be to audit production databases for abnormal database activity. The minimum level of audit is primarily used to gather some historical information about particular database activities and to detect specific security items. At this level, only selected actions will be audited, e.g., failed attempts to connect to a database and failed attempts to select, insert, update or delete data due to a lack of privileges. All privileged roles and activity assigned to Database Administrators (such as create, alter or drop database objects, roles or users) will be audited.

b. An audit report will be generated at predetermined intervals. All audit reports will be reviewed by the Security Manager, Customer Audit Manager and/or other designated County personnel. The

ISS Security Manager will also be responsible for purging the audit trail after the audit records are archived. Additional copies of the audit report can be provided to other staff as needed, such as the Palm Beach County Internal Audit Department. In addition to standard scheduled reports, the Security Manager and Customer Audit Manager shall have the ability to generate ad hoc audit reports. If any suspicious activity is detected, additional levels of audit will be enabled to focus on the specific area of concern.

c. Audit information shall include, at a minimum, the user that executed the statement, the action code (a number) that indicates the audited statement executed by the user, the object or objects referenced in the audited statement and the date and time that the audited statement was executed.

10.32 Security Issues

a. To protect the audit trail from unauthorized deletions, the DELETE ANY TABLE system privilege will be assigned only to Database Administrators. Changes made to the database audit trail will be detectable by INSERT, UPDATE and DELETE activities against the audit table.

b. Audit records generated as a result of object audit options set on the audit table can not be deleted from the audit trail except by individuals with Database Administrator privileges, and this class of privileges itself has protection from unauthorized use. As a final measure of protecting the audit trail, any operation performed while connected with Database Administrator privileges shall be audited in the operating system audit trail, if available.

All employees approved with Database Administrator privileges to the database being audited must read and sign a copy of the ISS Database Administration Services Security Policy.

Database Administration Services
Information Systems Services Department
Palm Beach County, Florida

DATABASE ADMINISTRATION SECURITY POLICY

As an employee of the Palm Beach County Board of Commissioners or any of its direct or indirect agencies, (herein referred to collectively as the EMPLOYER), I, the EMPLOYEE named below, agree as follows:

1. Unless I have express written permission or instructions from the EMPLOYER, I will not purge any database audit trails. Audit trails will be purged only after backing up that trail into a safe media such as tape or protected directory.

2. I understand that my DBA privilege does not include the right of unauthorized access to data.

1. I understand that it is my responsibility to protect the data and audit trails. Any suspicious activity will be reported to the EMPLOYER.

2. I understand that any deliberate or improper exercise of my responsibility and authority is subject to disciplinary action as indicated in the Palm Beach County Merit Rules and may also be a criminal offense punishable to the extent of the law.

Deleting and/or altering official records constitutes a third degree felony as Official Misconduct per F.S. 839.25 and a first degree misdemeanor as Falsifying Official Records per F.S. 839.13

This agreement becomes effective immediately upon signing. This policy supercedes all prior oral and/or written agreements with respect to this subject. This does not alter or intend to alter, any other contractual or employment agreements between the EMPLOYER and the EMPLOYEE.

I am aware of, and understand the aforementioned Database Administration Security Policies of Palm Beach County.

____
Employee Name (please print)

____ _________________
Employee Signature **Date**

____ _________________
Manager Signature **Date**

11.0 System Transaction and Audit Log Policy

11.1 Purpose:

To provide a minimum collection of log data that can be expected to be available on every internal system running a production application. This information will assist with problem resolution efforts and system restore operations, and will also be valuable in investigations of system penetration attacks and fraud investigations.

11.2 Policy Overview:

Automated chronological or systematic records of changes to data are essential to reconstruct previous versions of the data in the event of corruption. Such records are useful in establishing normal activity, in identifying unusual activity, and in the assignment of responsibility for corrupted data.

11.3 Policy Provisions:

11.31 Contents of Logs for Systems Running Production Applications

a. All computer systems running the IT Facility's production application systems, if capable, must include logs which record, at a minimum, the following data: (1) user session activity including User-IDs, log-in date/time, log-out date/time, and applications invoked; (2) changes to critical application system files; (3) additions and changes to the privileges of users; and (4) system start-ups and shut-downs.

11.32 Logs of User-Initiated Security Relevant Activities

a. To assure that users are held accountable for their actions on the IT Facility's production computer systems, one or more logs tracing security relevant activities to specific users must be securely maintained for a minimum of ninety (90) days. Application and/or database management system (DBMS) software must keep logs of user activities and statistics related to these activities which will allow them to spot and issue alarms reflecting suspicious business events. This information will be

11.33 Special Labeling For All Non-Production Business Transactions

a. Transactions used for auditing, testing, training or other non production purposes must be labeled and/or otherwise separated from transactions used for production processing. This will help ensure that the IT Facility's records are not improperly updated by non-production transactions. A mechanism to clearly separate auditing, testing, training, and non-production transactions from production business transactions must be in place. This separation will avoid both confusion and improper updates of computerized records.

11.34 Persons Authorized To View Logs

a. All system and application logs must be maintained in a form that cannot readily be viewed by unauthorized persons. Persons are unauthorized if they are not a member of the internal audit staff, systems security staff, systems management staff, or if they do not clearly have a need for such access to perform regular duties. Unauthorized users must obtain written permission from the data owner prior to being granted such access. The intention of this policy is to limit access to logs--both application and system logs--to only those persons who have a bona fide need to have such access.

11.35 Regular And Prompt Review Of System Logs

a. To allow proper remedial action, logs must be reviewed in a periodic and timely manner as defined by the owner.

11.36 Notification to Users About Logging of Security Violations

a. Users must be clearly informed which actions constitute security violations. Users must also be informed that such violations will be logged.

11.37 Clock Synchronization for Accurate Logging of Events on the Network

a. All computers connected to the County's internal network must have the current time accurately reflected in their internal clocks. Having synchronized clocks will assist system problem diagnosis and resolution, particularly for client/server and other systems involving interdependent hardware. Accurate clock time is also necessary for reliable event logging, automatic software updates, and other security-related activities. All clocks should be set to local standard time, and should be promptly changed to reflect daylight savings time. Whenever there has been a system crash, a power outage, an operating system upgrade, or some other event that might affect the clock, the clock should be promptly reset. Because computer clocks may lose or gain time over a period of operation, they should periodically be checked and reset as necessary.

11.38 Resistance of Logs Against Deactivation, Modification, Or Deletion

a. The effectiveness of logs in large measure is dependent on the mechanisms used to protect the integrity of the logs as well as the mechanisms used to generate the logs. Mechanisms to detect and record significant computer security events must be resistant to attacks. These attacks include attempts to deactivate, modify, or delete the logging software and/or the logs themselves.

11.39 Writing Logs to WORM (Write Once, Read Many) Storage Media

a. To prevent unauthorized alteration, production systems connected to the Internet must store all system logs on WORM storage media or similar technology approved by ISS. System logs and applications logs must not be resident on Internet-accessible computers. The objective of this policy is to safeguard the integrity of logs.

11.40 Required Retention Period for Logs

a. Computerized logs containing security relevant events must be retained for at least ninety (90) days. During this period, such logs must be secured so that they cannot be modified, and are only accessible by authorized persons.

11.41 Retention of Access Control Privilege Logs

a Computerized records reflecting the access privileges of each user of the IT Facility and/or County’s multi-user systems and networks must be securely maintained for a minimum of ninety (90) days.

12.0 UNIX Server Security

12.1 **Purpose:**

To provide specific guidelines for maintaining account security and auditing UNIX server security protocols.

12.2 **Policy Overview:**

This policy establishes requirements for maintaining password security, modifying system access, and monitoring system access. The primary UNIX directory is the *root directory*, also called the *root*. This directory is not subordinate to any other directory on the UNIX server. The root directory must be protected from unauthorized access. Only designated server administration personnel will be granted access to the root directory.

This policy is applicable to all staff members and contractors responsible for system administration of the UNIX servers of the IT Facility, the County departments, agencies, and constitutional offices.

12.3 **Policy Provisions:**

12.31 Password Security Guidelines

a. UNIX system administrators must use the following guidelines for creating and managing user accounts and passwords.

- Require that all users have their own accounts. Account usage must be monitored carefully with UNIX commands such as *who* and *last.*

- Require that all general user ID's not have the admin parameter set to "true." All users must be in the staff group.

- Ensure that all accounts have a password and that accounts not be validated unless a password has been established.

- Educate users on the need to select passwords carefully and to protect their passwords.

- Restrict use of the root account to genuine system administrator duties.

- Never unpack or test new software while running under the root account.

- Change the password of every account supplied with the UNIX system and delete any that are not needed.

- Disable user accounts after a predetermined period of inactivity.

12.4 Modifying System Access

12.41 *Superuser Account*

a. The *superuser* is a privileged account associated with the user name *root*. The superuser has complete access to all commands and files on a given UNIX system. Activities restricted to the superuser include the following:

- modifying the root directory for a process;
- changing file ownership;
- setting the system clock;
- increasing or decreasing resource usage limits;
- specifying the network interface; and
- shutting down the system.

b. The above activities, among others, require that the system administrator have superuser privileges. Because superusers are allowed unrestricted access to the system, their errors can have major consequences. Therefore, system administrators must perform routine work with a regular account, not with a superuser account. Furthermore, password security procedures must be rigorously applied for the superuser account.

12.5 Remote Root Login Approval

A user cannot remotely log into a system through the root directory. For example, when logging in remotely, a user must log into his or her account and then use the “su?” command. The su command makes the user a superuser or another user. However, prior approval from the Security Administrator is required to use this function.

12.6 SUID and SGID Programs

The use of the SUID and SGID programs can cause major problems. These programs change the user ID and group ID respectively and it is possible for a perpetrator to assume someone else’s identity including privileges. To guard against this threat, the security administrator or designated System Administrator must:

Allow only authorized Security Administrators to access these programs. A current list of these individuals is to be maintained by the Security Administrator.

Regularly (during off-hours) print a compete listing of all SUID and SGID files on the system and verify this list either manually or by shell script. If there is no current, valid reason for a given file to be SUID or SGID, modify the permission immediately.

Strictly prohibit the use of SUID or SGID shell scripts. Shell scripts allow *shell escapes* in which the user temporarily leaves the shell to execute another program. This leaves the system vulnerable to executing unauthorized programs while the user has root or other temporary privileges.

Examine the source code for all programs that accord SUID or SGID privileges. This is particularly important for public domain programs but should also be performed for purchased software.

Accord the minimum privileges necessary. It is often possible to create a special group and write a SGID program rather than writing a SUID program. Otherwise it may be possible to create a special user and change the user ID to that user rather than to the root. Reset the modified user ID or group ID to the original value as soon as possible.

12.7 Monitoring System Access

The Security Administrator or designated System Administrator must closely monitor system access. All system and audit logs will be backed up daily. The following logs will be reviewed regularly by the authorized Server Administrators:

a. **/etc/security/lastlog** - cords the latest login time for each user. This time is displayed whenever the user attempts to log in. It contains login information (date, time, IP address, etc.).

b. **/var/adm/sulog** - designates the name of log file that records all attempts to use su.

c. **/var/adm/wtmp** - contains information related to server logins and logouts. To keep control of the hard disk, the file must be purged periodically. Because this file is examined by the last command, purged /var/adm/wtmp file entries must be stored in readily available archives.

d. **/var/adm/utmp** - contains information concerning users that are currently logged into the server.

e. **/var/adm/messages** - used by syslog and holds important system messages such as unsuccessful login attempts.

f. **smit logs** - contain information about the SMIT system administration tool.

The Security Administrator shall perform the following tasks:

a **Assessment of Recent Login Activity** - regularly monitor recent logins of users. This will involve checking the wtmp file and printing the sessions of the specified users, including login name, the device name, the process ID, the login time, the elapsed time, and comments.

b. **Authentication Checks** - periodically check the internal consistency of the authentication database and check both the overall structure and internal field consistency of all components of the authentication database. Report all problems found.

c. **Integrity Check -** examine system files against the authentication database. Compare each entry in the file control database to the corresponding file in the file system. If the owner, group, or permissions are different, document the error messages and report the discrepancies to the security administrator.

12.8 Network Security Considerations

Trusted machines are banned from the network. The exception is in the case of a test server and production server which may "trust" each other for High Availability Configuration considerations. This configuration must receive prior approval from the Security Administrator.

No dial-in access to production servers will be permitted without authorization from the Security Administrator. Dial-in access should be limited to emergency circumstances only.

13.0 Network Access

13.1 Purpose:

The purpose of this policy is to establish procedures and requirements to ensure the appropriate access of information transported via Palm Beach County information networks.

13.2 Policy Overview:

All information transported over Palm Beach County's computer networks is considered and will be protected as an information resource of the Board of County Commissioners and/or the Enterprise Users of the IT Facility. It is the policy of the County to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information.

Accordingly, ISS will perform information systems risk assessments, prepare information systems security action plans, evaluate and approve information security products, and perform other activities necessary to assure a secure information systems network.

Network Administrators are responsible for functioning as information systems security coordinators. These individuals are responsible for establishing and documenting appropriate network monitoring processes, monitoring performance and control logs, and performing similar security actions for the networks they administer. They are also responsible for reporting all suspicious computer and network security-related activities to the ISS Director and Security Manager. Administrators also serve as local information security liaisons, implementing the requirements of this and other network systems security policies, standards, guidelines, and procedures.

13.3 Network Access Control:

13.31 Passwords

a. Access control for computer and communication systems must be achieved via passwords which are unique to each individual user. Access control to files, applications, databases, computers, networks, and other system resources via shared passwords (also called "group passwords") is prohibited. Passwords for desktop or laptop PCs must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, in computers without access control, or in other locations where this information could be gained by unauthorized persons. (See Section 6.0 "System Access Control.")

13.32 Log-In/Log-Off Process

a All users must be positively identified**,** with the exception of those devices provided for public access purposes, before access is permitted to any communications system resources. Positive identification for internal networks involves a User-ID and a fixed password, which are unique to an individual user. Where systems software permits, every log-in banner on multi-user systems must include a special notice. This notice must state: (1) the system is to be used only by authorized users, and (2) by continuing to use the system, the user represents that he/she is an authorized user.

b. Positive identification for dial-up lines involves the use of hand-held tokens, cryptographic challenge/response, or other approved extended user authentication techniques. The combination of a User-ID and a fixed password does not provide sufficient security for dial-up connections. Modems directly attached to network-connected workstations are forbidden because they do not provide adequate positive user identification. Modems connected to isolated computers (such as portable computers and home computers) are permissible.

c. Positive identification for users originating external real-time connections to the County's networks via value added networks, public networks (like Internet), or any other external communications system must also involve extended user authentication techniques.

d. The log-in process for network-connected systems must simply ask the user to log-in, providing prompts as needed. Specific information about the organization, the computer operating system, the network configuration, or other internal matters must not be provided until a user has successfully provided both a valid User-ID and a valid password.

e. If there has been no activity on a computer terminal, workstation, or microcomputer for a specified period of time (recommended for 15 minutes), the system must automatically blank the screen and suspend the session. Re-establishment of the session must take place only after the user has provided a valid password.

f. With the exception of electronic bulletin boards or other systems where all regular users are anonymous, users are prohibited from logging into any County system or network anonymously (for example, by using "guest" User-IDs). If users employ systems facilities which allow them to change the active User-ID to gain certain privileges, they must have initially logged-in employing a User-ID that clearly indicates their identity. On UNIX systems, this means that users must be prevented from initially logging-in as "root," but must instead first log-in employing their own User-ID. If such users have been granted the ability to achieve super user privileges, they may then "set userid" ("su") to gain "root" access. For all types of operating systems, logs must record all changes of current User-IDs.

13.33 Limiting System Access

a. The communications system privileges of all users, systems, and independently-operating programs (such as "agents") must be restricted on a need-to-know basis. This means that privileges must not be extended unless a legitimate business-oriented need for such privileges exists.

b. Controls must be in place to assure that access to computer systems is restricted to authorized users only. These restrictions can be implemented via routers, gateways, firewalls, front-end telecommunications processors, and other network components. These restrictions must be used to control "passthru" (i.e., where a user logging into a certain computer then moves from that computer to another device).

13.34 Process for Granting System Privileges

a. Requests for new User-IDs, IP Addresses and changed privileges must be in writing and approved by the user's manager in order for a network or systems administrator to fulfill these requests. To help establish accountability for events on the related systems, documentation pertaining to these requests will be retained for the period that the User ID remains active.

b. Third party vendors must NOT be provided dial-up privileges to the County’s computers and/or networks unless the involved Department Director determines they have a bona fide need. These privileges must be enabled only for the time period required to accomplish the approved tasks (such as remote maintenance or software development projects). If a perpetual or long-term connection is required, then the connection must be established by approved extended user authentication methods (hand-held tokens, software-based challenge/response process, etc.).

c. All persons wishing to use the County's internal networks, or multi-user systems must sign a compliance statement prior to being issued a User-ID (form attached). A signature on this compliance statement indicates the involved user understands and agrees to abide by the County's policies and procedures related to computers and networks (including the instructions contained in this document).

13.35 Process for Revoking System Access

a. If a computer or communication system access control subsystem is not functioning properly, it must default to denial of privileges to users. If access control subsystems are malfunctioning, the systems they support must remain unavailable until the problem has been corrected.

b. Users must not test, or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing by the ISS Director. Incidents involving unapproved system cracking (hacking), password cracking (guessing), file decryption, bootleg software copying, use of network monitoring or traffic capturing devices, or similar unauthorized attempts to compromise security measures might be unlawful, and will be considered serious violations of the County's security policies. Likewise, short-cuts bypassing systems security measures, as well as pranks and practical jokes involving the compromise of systems security measures are prohibited.

c. Management must promptly report all relevant changes in worker duties or employment status to the Security Administrators responsible for User-IDs associated with the involved persons.

13.36 Access Path Review, Approval and Changes

a. Changes to the County's internal networks include loading new software, changing network addresses, reconfiguring routers, and adding dial-up lines. With the exception of emergency situations, all changes to the County's information networks must be: (a) documented in a Customer Service Request (CSR) and/or a Change Request, and (b) approved in advance by ISS except as explicitly delegated by the ISS Director. Emergency changes to the County's networks must only be made by persons who are authorized by the ISS Director (or designee).

b. Workers must NOT establish electronic bulletin boards, local area networks, modem connections on existing local area networks, or other multi-user systems for communicating information without the specific approval of the ISS Director. New types of real-time connections between two or more in-house computer systems also require approval from ISS before the connects are established.

c. Participation in external networks as a provider of Internet or other electronic services that external parties rely on is prohibited, unless these conditions are fulfilled as follows: 1) the County Attorney's Office must identify the legal risks involved; 2) the Senior Manager of Data Communications Services must identify technical security risks; and 3) the ISS Director must expressly accept these and other risks associated with the proposal.

d. Sessions via dial-up lines connected to the County's internal networks and/or multi-user computer systems must pass through an additional access control point (firewall) before users employing these lines can reach a log-in banner. This policy applies to Internet inbound calls as well as Electronic Data Interchange (EDI).

e. Remote maintenance ports for the County computer and communication systems must be disabled until access is required by the vendor. These ports must be disabled immediately after use. Alternatively, dial-up connections can be established with vendors via outbound calls initiated by County workers. No firewall access control is needed for either type of connection.

f. Portable phones using radio technology as well as cellular phones must not be used for data transmissions containing County "confidential" or "restricted" information unless the connection is encrypted. Likewise, other broadcast networking technologies (i.e., radio-based local area networks) must not be used to transport sensitive information unless the link is encrypted. Such links may be used for electronic mail only if the content of the document is public information.

13.37 Handling Network Security Information

a. The Security Manager will periodically designate individuals to audit compliance with this and other computer and network security policies. At the same time, every worker must promptly report any suspected network security problem--including intrusions and out-of-compliance situations--to the ISS Solution Center.

b. All network or systems software malfunctions must be immediately reported to the ISS Solution Center**,** and the involved external information system service provider, if applicable. Ignoring these malfunctions could lead to serious problems such as lost or damaged information as well as unavailable network services.

c. Information about security measures for the County's computer and communication systems is confidential and should not be released to unauthorized persons. For example, publishing modem phone numbers or other system access information in directories is prohibited.

13.38 Physical Security of Computer and Communications Gear

a. All County network equipment must be physically secured with anti-theft devices if the equipment is located in an open office environment. Additional physical access control may also be used for these devices. For example, local area network servers must be placed in locked cabinets, locked closets, or locked computer rooms.

b. Access to communications wiring closets, computer machine rooms, network switching rooms, and other work areas containing "restricted" or "confidential" information must be physically restricted. Management responsible for the staff working in these areas must consult the Security Manager to determine the appropriate access control method (receptionists, metal key locks, magnetic card door locks, etc.).

c. "Restricted" or "confidential" information must not be downloaded to remote locations unless proper physical security and encryption facilities are installed and observed.

13.39 Exceptions:

a. The ISS Director acknowledges that special circumstances may require that certain users employ systems that are not compliant with these policies. All such instances must be approved in writing and in advance by the ISS Director (or designee).

14.0 Data Encryption

14.1 Purpose:

The purpose of this policy is to establish direction, procedures, and requirements to ensure the appropriate protection of data stored and transported by computer systems connected to the Palm Beach County network. Encryption is a technique or algorithm used to protect the confidentiality and integrity of data and provide authentication between the client and the server.

14.2 Policy Overview:

Encryption can be performed on stored information and transported information to protect it from unauthorized viewing. In some cases, encryption is used to protect passwords and restrict access to confidential data. It has more recently been used as a means of authentication, or proof of origination - ensuring that the functions of communications and system access are being performed by authorized individuals.

This policy does not address authentication. The level and type of encryption will depend on the nature of the information being protected and the system performance requirements.

14.3 General Policy:

All information transported over Palm Beach County's computer networks is considered and will be protected as an information resource of the Board of County Commissioners and/or the Enterprise Users of the IT Facility. It is the policy of the County to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information.

14.31 Encryption of Passwords

a. All system passwords must be encrypted when held in storage for any significant period of time or when transmitted over networks, to protect them from unauthorized disclosure. Passwords must be protected from exposure to "password collection" programs or network analysis devices.

14.32 Transmission of Sensitive Information

a. Encrypted confidential or classified information transmitted over the public network or private County network must use encryption facilities that have been approved by the Information Systems Security Committee.

14.33 Storage of Sensitive, Confidential or Restricted Information

a. All confidential information that is not being actively used must be stored in encrypted form. This also means that information stored on transportable storage media, such as magnetic tapes, diskettes and CDs, must be in encrypted form. When not in use, this media must be stored in a locked safe, locked furniture, or a similarly secured location.

b. Remote or portable systems storing confidential information must employ hard disk encryption systems. Users in the possession of portable, laptop, notebook, palmtop, and other transportable computers containing restricted or confidential information must not leave these computers unattended at any time unless the information is stored in encrypted form. These devices will also deploy a password protected screen saver with a launch time of no more than 5 minutes.

14.34 Commercially Available Encryption Products

a. Confidential information which is stored or transmitted must be encrypted via commercially available products approved by ISS. The Data Encryption Standard (DES) algorithm is recommended, but other algorithms will be considered upon request.

14.35 Downloading or Transferring Sensitive, Confidential or Restricted Information

a. Confidential information must not be downloaded to remote locations--such as home offices, other County buildings, or other offices--unless proper physical security and encryption facilities are installed and used.

14.36 Deletion of Sole Readable Versions of Information

a. Whenever encryption is used, the sole readable version of the information must not be deleted until the worker has first demonstrated the ability to decrypt the information into a readable version.

14.37 Restriction of Access to Encryption Keys

a Access to encryption keys must be strictly limited to those individuals identified by the ISS Director, the Information Security Committee, or the Enterprise Users of the involved data. Approval by the ISS Director, owners, or both will be necessary for encryption keys to be revealed to consultants, outside contractors or temporary staff. In addition, encryption keys must be encrypted when transported over the network. Encryption key management responsibilities will be explicitly assigned.

14.38 Encryption Key Management Process

a. Whenever such facilities are commercially available an automated, rather than manual, encryption key management process must be used for the protection of information on Palm Beach County’s networks.

14.4 <u>**Responsibilities**</u>:

a. ISS will obtain, install and maintain encryption technology as necessary to protect confidential, non-public information. ISS will provide technical training and assistance in the proper use of encryption software.

b. Assigned Enterprise Users will determine which specific data elements are confidential thereby requiring encryption for storage or transmission.

15.0 Virus Control

15.1 Purpose:

To establish a policy to minimize the risk of introducing viruses into County-owned computer systems and the IT Facility. It also provides guidelines for the detection and removal of viruses from computer systems.

15.2 Policy Overview:

A virus is a self-replicating program spread from executables, boot records, and macros. Executable viruses modify a program to do something other than the original intent. There are different levels of sophistication in how difficult a virus may be to detect.

The frequency that new applications or files are loaded on to the computer is proportional to the susceptibility of that computer to viruses. Configuration changes resulting from exposure to the Internet, exposure to mail, or receipt of files from external sources are more at risk for contamination. Viruses are normally introduced into a system by a normal act of a user (e.g., installation of an application, FTP of a file, reading mail, etc.).

The security policy for viruses has three aspects: 1) **prevention**: measures which prevent the introduction of viruses into a computing environment; 2) **detection**: determination that an executable, boot record, or data file is contaminated with a virus; and 3) **removal**: deletion of the virus from the infected computing system which may require complete reinstallation of the operating system, deleting files, or deleting the virus from an infected file.

15.21 Prevention

a. The following policies will apply with the objective of the spread of viruses:

- Only licensed and authorized applications may be installed on a computer. Software configurations will be scanned on a periodic basis to validate that no extraneous software has been added to a computer.

- Each department/agency shall maintain a listing of software approved for use by their employees.

- ISS shall maintain a list of standard desktop software products as well as a list of any specifically prohibited software products.

- ISS shall maintain a list of standard desktop software products as well as a list of any specifically prohibited software products.

- Software will be downloaded and installed only by authorized personnel who will scan or test the software.

- Anti-virus software will be installed on file servers to limit the spread of viruses within the network. Scanning of all files and executables will occur daily on the file servers.

- Desktop workstations will have memory resident anti-virus software installed and configured to scan data as it enters the computer. Programs will not be executed or files without prior scanning.

- All incoming mail and files received from across a network must be scanned for viruses as they are received. Virus checking will be performed if applicable at firewalls that control access to networks. This will allow centralized virus scanning for the entire County, and reduce overhead by simultaneously scanning incoming messages that have multiple destinations. It also allows for centralized administration of the virus scanning software, limiting the locations on which the latest virus scanning software and virus signature files need to be maintained.

- Employee security training will include the following information about virus infection risks: (1) new and more sophisticated viruses are being developed constantly; (2) virus scanning software must be updated by the System Administrator on a regular (monthly or quarterly) basis to maintain currency with the latest viruses; (3) the employee must inform the ISS Solution Center of any different or unusual behavior exhibited by a computer or application; and (4) the user must immediately discontinue operation of a computer that is infected, or thought to be infected, to reduce the risk of spreading or increasing the impact of a virus.

15.22 Detection

a. The following policies will apply for the detection of viruses:

- Virus-scanning tools will be used to scan computers on a daily basis. The tool will be updated on a monthly basis. All software or data imported onto a computer (from floppy disk, e-mail, or file transfer) will be scanned before being used.

- Virus scanning of all file systems on a daily basis is mandatory .

- When informed that a virus has been detected, the System Administrators will notify all users who may have access to the same programs or data that a virus may have also infected their system and then check these systems for viruses.

15.23 Removal

a. Any machine thought to be infected by a virus will not be used until after the system administration staff has verified that the virus has been removed. If the virus cannot be removed, all software on the computer will be deleted including boot records, if necessary. The software will then be reinstalled from uninfected sources and re-scanned for viruses.

16.0 Business Recovery Contingency Planning

16.1 **Purpose:**

The purpose of this policy is to ensure the appropriate Disaster Recovery and Business Contingency Plans are developed and implemented to protect the mission-critical computer systems and applications of the IT Facility and the County.

16.2 **Policy Overview:**

To ensure proper Disaster Recovery and Business Contingency planning, all County agencies with mission-critical information systems must develop and implement a Recovery Plan. Prior to installing a mission-critical application into production, the Recovery Plan must be in place.

16.3 **Recovery Plan:**

Recovery Plan provisions are required to permit a County agency to continue essential functions if automated information technology support is interrupted. The Plan will be coordinated with any separate policies or procedures for backups, hot site testing, and contingency plans of mission-critical systems. This Plan must include Networks or Internet Web services used by the application. The Plan provisions will ensure that interfacing systems are identified and disaster/contingency plans coordinated.

16.4 **Plan Provisions:**

The Recovery Plan will include the following provisions for policies, procedures, standards and operational instructions.

a. Executive Overview with a Plan summary, assumptions and a simple definition to identify a disaster situation.

b. Plan Strategy will identify the processes from the time of a reported disaster situation through to the resumption to normal business operations.

Successful recovery of the operation will include procedures to:

. Distribute updated Recovery Plans to appropriate personnel
. Train personnel on all aspects of the Recovery Plan
. Integrate Plan with security measures and internal controls
. Perform comprehensive test of Plan (Hot Site Plan)
. Modify the plan as a result of the test
. Safeguard vital records
. Backup data and store media off-site

c. List of mission-critical applications, business functions and all information technology resources required for recovery to a normal state of business.

d. Call list of team members required to support the Recovery Plan. If organized into teams, a separate Team Task/Assessment checklist of team members and associated responsibilities and instruction for each member will be prepared. Team members representing Enterprise Services, Applications, Networks, Data Base Administration, Server and Desktop Administration, and Security must be included in the Plan.

e. Restore procedures - will be the most detailed section of the Recovery Plan. The following topics must be defined in detail:

- Business Recovery Preparation List - describes the actions required for the separate Alert Level (Watch, Warning or Disaster)
- Off-Site Away Plan - a detailed action plan with objectives defined by checkpoints on the schedule processes
- Business startup list and Network recovery
- Personnel Schedule for Hot Site recovery
- Support Personnel List
- Equipment Shutdown list for Networks, Server and Enterprise processors
- Production Schedule checklist for recovery

f. Hot Site and Plan Testing - will identify and document procedures for testing the Recovery Plan in a controlled and scheduled environment. The Hot Site Plan will have a predefined list of critical systems to test with scripts, test team organization chart**,** and Hot Site Task Checklist for all members involved in the test. The emphasis on the Hot Site Test is to annually exercise the Recovery Plan and modify the plan from test results. Off-site testing of the Hot Site test plan may not be economical or practical for all applications.

g. Plan Maintenance - will define the activity necessary to maintain the Recovery Plan. Plan Maintenance is of the utmost importance to assure on-going relevance to what is to be recovered and procedures governing the recovery. In addition to the Plan review, recovery data, backups and materials stored off premises will be inventoried and assessed periodically.

h. Appendix - additional procedures and information to be included, if not addressed above:

- Employee Directory
- Vendor by Name Report
- Software by Description Report
- Equipment List
- Supply Report
- Data Communication Report
- Vital Records Report
- Location Report
- Media Interface
- Notification to Key Executives, EOC Staff
- Hot Site Information
- Current Environment
- Backup Procedures
- Offsite Storage Information

16.4 Contingency Planning (All Agencies):

A Contingency Plan for automated systems must be maintained by the Enterprise User to include a detailed procedure to maintain information in a manual mode in the event that the disruption of automated services are extended for any length of time. This plan must assign responsibility and define operational instructions to collect, update and report information in a manual mode, or document a determination that the County will not be able to perform that process until the automated systems are restored.

16.5 Business Recovery Assessment:

ISS shall contract with an outside vendor for assistance with disaster recovery and **“**Hot Site**”** operations for the County’s designated mission-critical systems.

16.6 Information System And Services Support:

Enterprise Users responsible for developing a Disaster Recovery Plan should contact ISS to review a sample of a comprehensive Disaster Recovery Plan for mission-critical systems.

17.0 Back-up, Storage and Destruction of Data

17.1 Purpose:

The purpose of this document is to outline the policies and procedures for insuring frequent, reliable and useable copies of transactions and data in the event production systems or data become inaccessible for any reason.

17.2 Policy Overview:

Backups are performed on a regular basis in compliance with state and County regulations, and as specified in the system support documentation, or system administration procedures. System backups may involve entire volumes or subsets of data. The application Enterprise Users (or their designees) are responsible for establishing standard schedules for backup and retention activities. ISS is responsible for performing backups on enterprise systems and servers. However, each department/agency is considered the “Enterprise Users of its records and has the responsibility for maintaining “record master” copies. The Department Director is responsible for assuring that adequate backup procedures are established for any server or system which is administered by the Department.

All backups will be tested with a restore operation after the initial installation, upgrade or major change to the environment or data. Automated backup operations need to be examined on a regular basis for successful completion. As an additional precaution, all backup media will be stored offsite in a secure, environmentally approved facility. The objective is to ensure recoverability of the systems should a disaster or business interruption prohibit access to the production computer facility. Backup tapes and media will be eligible for recycling following a one year retention, unless otherwise specified. Data destruction and deletion of obsolete data sets are the responsibility of the individual user, with appropriate management approval.

17.21 Destruction Of Records Or Information Requires Management Approval

a. Users must not destroy or dispose of potentially important County records or information without specific and prior management approval. Unauthorized destruction or disposal of County records or information will subject the perpetrator to disciplinary action up to and including termination and prosecution. Records and information must be retained if: (1) they are likely to be needed in the future; (2) regulation or statute requires retention, or (3) they are likely to be needed for the investigation or prosecution of unauthorized, illegal, or abusive acts.

17.22 Backup Security Administrator Must Be Designated And Trained

a. Each computer with an access control system will have a designated employee who will be responsible for User-ID assignment, user access privilege control, and designated “Systems Administrator.”

Each applicable department and agency should also train at least one other employee to assume these duties when the System Administrator is absent from work.

17.23 Backup Schedules and Content

a. All critical business information and critical software residing on the County's computer systems must be periodically backed-up as required by the owners/customers. These backup processes will apply to production systems and must be performed with sufficient frequency to support documented contingency plans.

b. Backups are performed daily, weekly and monthly. Unless otherwise specified in writing, the following backup and retention schedules are in effect within ISS.

- **Daily Backups**

Mainframe**:** backups performed nightly (M-F) with a retention period of 10 working days. These backups are picked up by the off-site storage vendor the following morning and are stored off site for five working days. Upon return, these records remain in the tape library for an additional five working days to reach the 10-day retention period.

Database: backups performed nightly (M-F). Sites that have weekend activity should also run backups on weekend nights (S-S). These backups are retained for a minimum of one week, and they are not rotated off-site.

Office
Automation: Office Automation servers will be backed up nightly (M-F). These backups are retained for a minimum of two weeks.

- **Weekly Backups**:

Mainframe: There is a one month retention for weekly backups, to be performed on Saturday and Sunday. Backup tapes are sent to the County's offsite storage vendor on Monday where they are kept for one week and returned to the ISS' tape library for the remaining three weeks of retention.

Database**:** Backups are retained for a period of three weeks and are retained on-site.
Office Automation: Backups are retained for a minimum of a two month period. The most recent weekly full backup is rotated off-site.

- Monthly Backups:

Mainframe: Monthly backups are controlled by the hierarchical storage management (HSM) program, and upon creation are forwarded to the off-site storage vendor for one week and then returned to the ISS tape library where they are retained for the remainder of 16 months.

Database: Monthly tape backups are retained for a minimum of one year.

Office Automation: Monthly tape backups are to be retained for a minimum of six months.

c. **Critical Records to be Identified by Department and Agency Managers**

- Department and Agency managers must identify and maintain a current list of the critical records needed to restore operations following a disaster or system outage. Criteria which organizations may use to identify critical records include: information needed to conduct routine business transactions, information needed to recreate the County's financial and legal position, and information required to preserve the legal rights of the public.

d. Two Copies of Critical County Records Stored Off-Site

- At least two recent and complete backups (not incremental backups) made on different dates containing critical County records must be stored off-site. A second copy is to be maintained as insurance in case one set of records is damaged or deleted during a restore operation or due to some unforeseen circumstances. Another objective of this policy is to dictate a backup media rotation process (sometimes called "grandfather/father/son rotation") that involves at least two off-site copies.

e. **Encrypting Backup Media Stored Off-Site**

- To prevent records from being accessed by unauthorized parties, all sensitive, valuable, or critical information recorded on backup computer media (magnetic tapes, floppy disks, optical disks, etc.) and stored outside the County offices must be in encrypted form. Whether encryption is appropriate must be determined and the justification documented by the user based on the nature of the records.

f. **Supplementary Backups Required For Desktop and Portable Computers**

- Following the departmental policy for data storage, workers using these computers and storing critical information on local hard drives must make regular backups. In addition, these separate backup copies should be made each time changes are saved. These backups should be labeled and stored in a central location, cataloged for easy identification and retrieval.

g. **Management Review Of End-User Backup Process**

- Department managers or their delegates must ensure that proper backups of sensitive, critical and valuable data are being made if such data resides on personal computers, or other small systems.

h. **Data Storage Media**

- Only reliable data storage media will be used for backup purposes. Old and worn storage media cannot be relied upon to accurately preserve information. Computer media storage procedures must assure that sensitive, critical, or valuable information stored for prolonged periods of time is not lost due to deterioration of the storage medium. For instance, management must copy data to different storage media if the original backup media is showing signs of undue deterioration.

i. **Directory of Backup Data and Locations**

- Records of all archival backup data stored on-site or off-site must be maintained in an up-to-date directory showing the date when the information was most recently modified as well as a description of the information category. The directory of the files and their locations might be automatically generated as a by-product of the system's activity. These directories might also be maintained manually, although both the level of effort and the propensity to make errors is much higher with a manual system. This directory will be used in the event that system or data restoration becomes necessary.

j. **Off-Site Storage Of Backup Media**

- Backups of essential information and software must be stored in an environmentally-protected and access-controlled site which is a sufficient distance away from the originating facility to mitigate risks from a natural disaster.

17.24 __**Retention Requirements**__:

a. **Minimum Information Retention Period**

- Information listed on the Information Retention Schedule must be retained for the period specified. Other information must be destroyed when no longer needed--generally within two years.

b. **Responsibility For Archival Storage Data Retention Schedule**

- All County information must be securely retained according to a schedule developed and published by the custodian of the information. Retention periods will be established based on legal requirements, data sensitivity, criticality of the data and value of the data.

c. **Database Log Files**

- Online Transaction Processing or user updateable production databases containing original non-producible data will operate with archiving enabled. This will provide a backup of all changes to production data. As log files fill they will be archived to disk and later copied to tape. Archive log files will be mirrored to ensure availability of the log in case one file becomes unusable due to hardware malfunction. It will not be necessary to update read only or other databases which contain only reproducible or replicated data from other sources with achieving enabled.

- Some production databases will be mirrored for complete redundancy. Mirroring of the archive log files will not be enabled when the entire database is mirrored.

d. **File Restoration Processes**

- To reduce the possibility of unauthorized access to data, only designated administrators will be allowed access to file backups. Security Administrators will periodically check logs indicating which users restored which files to determine whether unauthorized activity has taken place.

e. **Destruction of Data**

- Destruction of data refers to the deletion of obsolete or otherwise unnecessary data. Data can be considered for destruction if it meets any of the criteria listed below:

old backups - backup tapes become eligible for re-use after one year. At that point, they may be over-written by current backup processing.

obsolete data sets - data sets no longer used by the application itself, or by the programming staff, are candidates for deletion. Typically, these are located on disk. They may be data sets left behind from an earlier release, test data sets that are no longer used, etc. The disposition of such data sets is approved by the individual owner of the specific data or their designee.

f. Destruction of Information on Used Equipment and Media Provided to Third Parties

- Before information systems equipment or storage media which has been used by Palm Beach County is transferred to any third party, all sensitive information must be removed. Department managers are responsible for verifying that appropriate precautions are taken to remove sensitive and confidential information from all media.

18.0 Change Control Management

18.1 Purpose:

To control changes relating to production computer and network systems administered by the Information Systems Services (ISS) Department. The change control policy and procedures must be used to manage all system modifications through documenting, tracking, approving, notifying and reporting all changes made to hardware, software, network and environments affecting the production information systems.

A *production system* is defined as any system or environment supporting or performing business functions. This includes all hardware, system software, applications software, data files, network, environmental equipment and procedural modifications.

18.2 Policy:

It is the policy of the ISS Department that plans, procedures and schedules for production system changes are to be documented and communicated to the affected areas within ISS and all affected County agencies, departments and constitutional offices. Documentation reflecting all changes to the production environment must be prepared prior to the time that a change takes effect. This documentation must describe the proposed change, impact of the change, the back out plan and management approval. For emergency changes, documentation must be completed as soon as possible after the change has been made.

All service areas in ISS shall follow change control guidelines when requesting changes to the production systems.

18.3 Procedures:

The change control procedure must be instituted for all significant changes to the production environment. An automated tool is used by ISS to manage the change process.

18.31 Formal Notification

a. Any change request must be submitted in writing. Formal notification is required for the purpose of planning, communicating, recording, coordinating schedules and resources, analyzing the change impact, and documenting a contingency plan. Examples of changes which must follow this process include modifications of technical infrastructure, hardware and software upgrades, implementation of new applications or databases, relocation of systems or users, etc. Requests from customers or a reported problems could trigger the need to make such a change.

18.32 Plan Documentation

a. It is the responsibility of ISS to provide a plan for the change. The change would identify the three phases of the plan (test, implementation and back out). ISS is responsible for assessing and communicating the risk and the impact of the request. The impact of the change will identify the actual and potential customers affected, the duration of the potential impact and the other systems or applications to be considered. The change requester may also spawn notifications to other staff and managers for better coordination and documented participation in the plan.

18.33 Risk Assessment

a. The risk of the change corresponds to the impact and complexity associated with the change. The materiality of the risk will determine which level of management must approve the change. Changes deemed as high risk require the approval of the Division Director. Medium risk changes can be approved by the Section Manager and low risk changes approved by assigned staff. Definitions of the three risk levels as follows:

- **high risk:** A high risk change affects more than one department, or impacts a system which is considered high risk**.** Another indicator of a high-risk change is any change which requires significant effort for back out and recovery. In addition, it may require special resources or scheduling. The Division Director must be notified for his or her approval at least three working days prior to implementation and presentation to the Change Schedule Team (CST).

- **medium risk:** Medium risk changes carry a moderate amount of exposure and complexity. It is a change that affects at least one department, but only requires a moderate effort for back out recovery. The Section Manager must authorize approval at least three working days prior to implementation and presentation to the CST.

- **low risk:** Low risk changes are routine modifications which carry low impact and complexity. The applications and individuals affected are limited, and minimal effort is required for back out and recovery.

18.34 Approval and Scheduling Process

a. Approval must be obtained prior to presenting the change at the CST meeting. When a requested change has been approved by the Division Director or Manager, final scheduling will be determined by the CST in order to avoid scheduling conflicts. All medium and high risk change requests for a production environment should be directed to the CST. For scheduling low risk impact changes, guidelines must be defined by the Section Manager.

18.35 Completion of Planned Changes

a. Upon completion of a planned change, there will be a confirmation that the change has been successfully implemented. After verification, the change record will be updated and completed. If the change is unsuccessful, the change record will be updated with the appropriate information, including confirmation of successful reversal of the change. Unsuccessful changes will require modifications to the plan and other change documentation, as well as the need to reschedule.

18.36 Emergency Changes

a. If required to resolve an existing or potential problem, changes may be exempt from the formal change management process. If the change request repairs an existing problem, the Change Control Management record must reference the problem report number. Emergency changes must be documented in the Remedy system.

b. The Section Manager is responsible for confirming that the emergency change is completed successfully with minimal impact to the environment. The Manager must notify all affected parties.

19.0 Reporting Security Incidents

19.1 Purpose:

This policy and procedure memorandum describes the steps which are to be followed for reporting physical and computer security incidents which occur within the ISS facility. The physical security incidents addressed in this procedure include theft, illegal building access, and property destruction. The computer security incidents covered in this procedure include suspected illegal system access (including account sharing), suspected computer break-in (both internal and external) and computer viruses.

19.2 Policy Overview:

One component of an effective security program is the tracking and reporting of security incidents. The document is intended to provide Palm Beach County technical support personnel with guidance for responding to security incidents. The term "incident" for purposes of this policy is defined as any irregular or adverse event that has the potential to impact the security of information technology resources. Examples of possible incident categories include: compromise of system integrity; denial of system resources; illegal access to a system (either a penetration or an intrusion); malicious use of system resources, or any kind of damage to a system. Some possible scenarios for security incidents include:

a. a “strange" process is running and accumulating large portions of CPU time;
b. an intruder is discovered logged into the County's system;
c. a virus has infected a County-owned system; or
d. it is determined that someone is trying to penetrate the system from a remote location.

19.3 Policy Provisions:

Handling a security incident involves determining the impact of the security violation, containing and eradicating the problem, notification of appropriate personnel, and the follow-up analysis.

A computer security incident may occur at any time of the day or night. If the first person on the call list to be notified can not respond within a reasonable time frame, then a secondary contact must be called in addition to the first. It will be the responsibility of the persons on the call list to determine if they can respond within a reasonable time frame.

19.4 General Procedures:

This section outlines procedures that are common for all types of security incidents.

a. **Documentation of Reported Incidents**
Logging of information is critical in situations that may eventually involve security violations, either accidental or intentional. The implications from each security incident are not always known at the beginning of, or even during, the course of an incident. Therefore, a written log will be kept for all security incidents that are under investigation. The information will be logged in a location that can not be altered by others. The type of information that will be logged includes:

- dates and times of incident-related phone calls and meetings;
- dates and times when incident-related events were discovered or occurred; amount of time spent working on incident-related tasks;
- individuals contacted; and
- identification of systems, programs or networks that have been affected.

b. **Notification of the ISS Security Manager**
It is extremely important that the appropriate individuals be made aware of security incidents. The ISS Security Manager is to be notified when a security violation is suspected or known. The Security Manager will document the reported incident and determine, based on the nature of the event, whether the ISS Department Director, the County Administrator, and the County Auditor should be notified.

c. **Release of Information**

It is important that information be controlled during the course of a security incident or investigation of a possible incident. All release of information must be authorized by the ISS Director or the County Administrator. All requests for public records should be forwarded to ISS Director.

d. **Follow-up Analysis**

After an incident has been fully investigated and affected systems restored to a normal mode of operation, a follow-up analysis should be performed. All involved parties (or a representative from each group) should meet and discuss actions that were taken and the lessons learned. All pertinent security procedures should be evaluated and modified, as necessary. All on-line copies of tampered files should be removed from the system(s) and stored in accordance with the Backup, Storage and of Destruction of Data section. If applicable, recommendations should be presented to the appropriate management levels. A security incident report should be prepared by the ISS Security Manager and distributed to all appropriate personnel.

20.0 Internet Usage

20.1 **Purpose:**

To establish policy for the appropriate use of the Internet as a resource for County agencies.

20.2 Policy Overview:

The Internet serves as a vast source of information and has quickly evolved into a powerful communications tool. Internet connectivity is critical to County agencies as well as members of the public who wish to obtain information about local government issues, projects and services.

Governmental organizations are increasingly using the Internet to increase productivity, improve the quality of services, and provide open access to public records. Conversely, unrestricted use of the Internet has the potential to adversely affect, rather than enhance productivity.

It is the general policy that Internet services are to be used in a responsible, efficient, ethical, and legal manner to support the programs of Palm Beach County. This policy addresses those specific authorized and restricted uses of the Internet when operating County provided equipment and/or access. It is applicable to all County employees as well as volunteers and contractors authorized to use County-owned equipment and facilities. It further specifies those administrative actions that can be taken in the event an employee is found in violation of the policy.

All desktop and laptop computers assigned to Board employees are configured to provide unrestricted Internet access. Usage of the Internet may be subject to review and audit to ensure compliance with this policy.

20.3 **Policy Provisions:**

This policy applies to all employees using computers or Internet connections supplied by Palm Beach County, from any location during working and non-working hours. This policy also applies to contractors and volunteers who are authorized to use County-owned equipment and facilities to access the Internet. It is the general policy that Internet services are to be used in a responsible, efficient, ethical, and legal manner to support the programs of Palm Beach County government. The Use, Retention, and Destruction of Electronic Mail (e-mail) is addressed in a separate Policy and Procedure Memorandum (PPM #: CW-R-006).

20.31 Unacceptable Activities

a. County employees are specifically prohibited from accessing the Internet for the purposes of engaging in the following activities:

b. receipt and dissemination of sexually explicit, hate oriented, threatening or illegal images or information, including offensive jokes or cartoons;

c. accessing any web site that promotes discrimination, hatred, or religious intolerance;

d. gambling;

e. promoting or endorsing an outside business venture;

f. non work-related chat rooms;

g. engaging in unauthorized fund raising efforts or political activities (any fund raising effort utilizing the Internet must be explicitly approved by the County Administrator); and

f. downloading illegal or "pirated" software, audio, or video files.

The above is not an all-inclusive list of prohibited Internet usage. Accessing inappropriate web sites and activities that would reflect unfavorably on the County and it's various organizations, employees, and citizens is strictly prohibited. This includes, but is not limited to, sexually explicit web sites and chat rooms as well as any web site that promotes discrimination or hatred.

20.32 Acceptable Uses for Non-Business Purposes

a. Limited use of the Internet for non-business purposes may be permitted in accordance with individual department policies. Any usage of the Internet for non-business purposes must conform to the following requirements:

(1) use does not include any of the unacceptable activities listed above;

(2) use occurs within the employee's personal time (i.e., lunch break,

scheduled break periods, before and after work, weekends) or flex-time; and

(3) use is restricted and scheduled so as not to infringe upon the employee's duties and work productivity.

b. Examples of permissible use for non-business purposes include: personal correspondence, monitoring of the deferred compensation program, and job hunting.

20.33 Security Issues

a. County employees must be aware of the security threats posed by use of the Internet. Security threats may be introduced to the Palm Beach County computing environment by sending or receiving information through the Internet. The threat can be in the form of viruses (attached to documents or downloaded software) that are designed to corrupt data bases and/or direct attack by hackers with the intention of accessing sensitive information or disrupting the operations of the County**.** A secure firewall will be administered by ISS to protect against the threat of outside intruders who may be attempting to gain unauthorized access to County systems and data. ISS will also identify and license for the County, an approved virus screening program to be placed on all computers (regardless of Internet access).

b. Files containing confidential County data, as defined by existing security policies, must be encrypted if these files are transmitted through the Internet. Each agency sending data over the Internet is responsible for determining whether encryption is appropriate.

20.4 <u>Responsibilities</u>

Primary responsibilities relating to Internet access and use are outlined below.

a. ISS:

(1) establish the County policy on Internet activity

(2) identify and block access to unacceptable web sites

(3) provide Internet access to authorized users

(4) administer the Internet security function to include firewall protection

b. User Departments and Agencies:

(1) authorize access to Internet for their employees
(2) establish departmental policy on non-business use of the Internet
(3) monitor program for compliance
(4) take positive corrective action upon notice of violation
(5) ensure virus scanning software is installed on each PC workstation