Oklahoma County

Information Security

Information Security Policy, Procedures, and Guidelines

TABLE OF CONTENTS

PREFACE

The contents of this document include the minimum Information Security Policy, as well as procedures, guidelines and best practices for the protection of the information assets of Oklahoma County (hereafter referred to as the County). The Policy, as well as the procedures, guidelines and best practices apply to all Offices and Departments utilizing the Board of County Commissioners (BOCC) network. As such, they apply equally to all County employees, contractors or any entity that deals with County information.

The Management of Information Systems (MIS) department of the BOCC will communicate the Policy, procedures, guidelines and best practices to all County Offices and Departments. In turn, all Offices and Departments are required to review the Policy and make all staff members aware of their responsibility in protecting the information assets of the County. Those Offices and Departments that require additional controls should expand on the content included in this document, but not compromise the standards set forth.

The Policy and those procedures prefaced by "must" are mandatory as the system involved will be classified as insecure without adherence. Guidelines and best practices are generally prefaced with "should" and are considered as mandatory unless limited by functional or environmental considerations.

It is recognized that some Offices and Departments have their own proprietary systems that may not conform to the Policy, procedures, guidelines and best practices indicated in this document. A plan for resolution of these system limitations should be created. Any exceptions are to be documented and be available on request. Other non-system related standards that do not require system modification should be instituted as soon as possible.

Revisions to this document are maintained collectively in Appendix E: Revisions, which includes a "Revision Table" describing each addition, change or deletion and the date it was implemented. All revisions are referenced using this procedure. The original document will remain intact.

Oklahoma County

INFORMATION SECURITY POLICY

Information is a critical County asset. Information is comparable with other assets in that there is a cost in obtaining it and a value in using it. However, unlike many other assets, the value of reliable and accurate information appreciates over time as opposed to depreciating. Shared information is a powerful tool and loss, or misuse can be costly, if not illegal. The intent of this Security Policy is to protect the information assets of the County.

This Security Policy governs all aspects of hardware, software, communications and information. It covers all County Offices and Departments as well as contractors or other entities who may be given permission to log in, view or access County information.

Definitions:

- *Information includes any data or knowledge collected, processed, stored, managed, transferred or disseminated by any method.*
- *The Owner of the information is the County Office or Department responsible for producing, collecting and maintaining the authenticity, integrity and accuracy of information.*
- *The Hosting County Office or Department has physical and operational control of the hardware, software, communications and databases (files) of the owning Office or Department. The Hosting Office or Department can also be an Owner.*

The confidentiality of all information created or hosted by a County Office or Department is the responsibility of that County Office or Department. Disclosure is governed by legislation, regulatory protections and rules as well as policies and procedures of the owning County Office or Department. The highest of ethical standards are required to prevent the inappropriate transfer of sensitive or confidential information.

All information content is owned by the County Office or Department responsible for collecting and maintaining the authenticity, integrity and accuracy of the information. The objective of the owning County Office or Department is to protect the information from inadvertent or intentional damage, unauthorized disclosure or use according to the owning Office's or Department’s defined classification standards and procedural guidelines.

Information access is subject to legal restrictions and to the appropriate approval processes of the owning County Office or Department. The owning County Office or Department is responsible for maintaining current and accurate access authorities and communicating these in an agreed upon manner to the security function at the County Office or Department hosting the information. The hosting County Office or Department has the responsibility to adhere to procedures and put into effect all authorized changes received from the owning County Office or Department in a timely manner.

Information security – The County Office or Department, who collects and maintains (owns) the information, is responsible for interpreting confidentiality restrictions imposed by laws and statutes, establishing information classification and approving information access. The hosting County Office or Department will staff a security function whose responsibility will be operational control and timely implementation of access privileges. This will include access authorization, termination of access privileges, monitoring of usage and audit of incidents. The County Office or Department that access the systems have the responsibility to protect the confidentiality of information which they use in the course of their assigned duties.

Information availability is the responsibility of the hosting County Office or Department. Access to information will be granted as needed to all County Offices or Departments to support their required processes, functions and timelines. Proven backup and recovery procedures for all data elements to cover the possible loss or corruption of system information are the responsibility of the hosting County Office or Department.

The hosting County Office or Department is responsible for securing strategic and operational control of its hardware, software and telecommunication facilities. Included in this mandate is the implementation of effective safeguards and firewalls to prevent unauthorized access to system processes and computing / telecommunication operational centers. Recovery plans are mandatory and will be periodically tested to ensure the continued availability of services in the event of loss to any of the facilities.

Development, control and communication of Information Security Policy, Procedures and Guidelines for Oklahoma County is the responsibility of MIS. This Policy represents the minimum requirements for information security at all County Offices and Departments. Individual Office or Department standards for information security may be more specific

than these County-wide requirements but shall in no case be less than the minimum requirements.

1.0 INTRODUCTION

1. This document states the Policy and outlines procedures, guidelines and best practices required for creating and maintaining a secure environment for the storage and dissemination of information.

2. It is critical that all Offices, Departments, and their staff are fully aware of the Policy, procedures, guidelines and best practices and commit to protecting the information of the County. Common sense and high ethical standards are required to complement the security guidelines.

3. The Policy, procedures, guidelines and best practices outlined represent the minimum security levels required and must be used as a guide in developing a detailed security plan and additional policies (if required).

1.1 BACKGROUND

1. The information Policy, procedures, guidelines and best practices apply to all Departments and Offices and are inclusive of their hardware facilities, software installations, communication networks / facilities as well as information.

1.2 POLICY, PROCEDURES, GUIDELINES

1. MIS has, among other responsibilities, the mandate to establish minimum mandatory standards for information security and internal controls as well as contingency planning and disaster recovery.

1.3 AUDIENCE

1. The Policy, procedures, guidelines and best practices are for distribution to all County Offices and Departments through their respective Security Representative who will then be responsible for communicating the details to County employees as well as contractors or other entities whose position responsibilities include the creation, maintenance, or access of County information residing on any computer system or platform. Appendix C assigns

the primary responsibility of the procedures, guidelines and best practices to the User, Owning Office or Department, or Hosting Office or Department.

2.0 INFORMATION

1. Management of information requires a working set of procedures, guidelines and best practices that provide guidance and direction with regards to security. The primary focus is on the confidentiality and integrity of the information required for delivering information throughout the County.

2.1 INFORMATION CONFIDENTIALITY

1. The overriding premise is that all information hosted or created by a County Office or Department is property of the County. As such, this information will be used solely for performance of position related duties. Any transfers or disclosures are governed by this rule.

2. The confidentiality of all information created or hosted by a County Office or Department is the responsibility of all County Offices and Departments. *Disclosure is governed by legislation, regulatory protections, rules as well as policies and procedures of the County and of the owning County Office or Department.* The highest of ethical standards are required to prevent the inappropriate transfer of sensitive or confidential information.

3. *Release of information is strictly for job related functions. Confidentiality is compromised when knowingly or inadvertently, information crosses the boundaries of job related activities.*

4. Users must be required to follow good security practices in the selection and use of passwords. Passwords provide a means of validating a user's identity and thereby establish access rights to information processing facilities or services. All County staff must be advised to:

   (A) keep passwords confidential,
   (B) avoid keeping a paper record of passwords, unless this can be stored securely,
   (C) change passwords whenever there is any indication of possible system or password compromise,
   (D) select quality passwords with a minimum length of twelve characters which are:
      (i) easy to remember,

(ii) not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers and dates of birth etc.,
(iii) free of consecutive identical characters or all-numeric or all alphabetical groups,

(E) change passwords as needed,
(F) avoid reusing or cycling old passwords,
(G) change temporary passwords at the first log-on,
(H) not include passwords in any automated log-on process, e.g. stored in a macro or function key, and
(I) not share individual user passwords.

2.2 INFORMATION CONTENT

1. All information content hosted by a County Office or Department is owned by and is the primary responsibility of the County Office or Department responsible for collecting and maintaining the authenticity, integrity and accuracy of information. The objective of the owning County Office or Department is to protect the information from inadvertent or intentional damage as well as unauthorized disclosure or use according to the classification standards and procedural guidelines of the owning County Office or Department.

2. The following procedures must be followed by all County Offices and Departments:
   (A) All information content must reflect the actual state of affairs of the respective County Office or Department.
   (B) Changes in the status of personnel who have system access are entered in the system immediately and the appropriate authorization / change form sent to the hosting agency's Security Administration.
   (C) In the event of a dismissal, the respective Agency is to call and notify the hosting agency's Security Administration immediately.

2.3 INFORMATION ACCESS

1. Information access is subject to legal restrictions and to the appropriate approval processes of the owning County Office or Department. The owning County Office or Department is responsible for maintaining current and accurate access authorities and communicating these in an agreed upon manner to the security function at the County Office or Department hosting the information.

2. All Offices and Departments must designate a security representative whose role includes:
   (A) communicating the Information Security Policy to all their respective employees,
   (B) communicating the appropriate procedures, guidelines and best practices to the responsible user, owner, or people directly responsible for hosting activities as indicated in Attachment C,
   (C) granting, on behalf of their Office or Department, user access to system functions, and
   (D) reporting all deviations to the Policy, procedures, guidelines and best practices.

3. Procedures for the Security Administration function at the Hosting Office or Department are:
   (A) Confirm set up to the Office or Department and the individual concerned via email when the set-up is complete for the role of Security Representative.
   (B) Confirm set up to the Security Representative and the individual concerned when the set-up is complete for the use roles assigned. The email confirmation will include access rights assigned in the system.
   (C)
   A daily report will be run by the Owning Office or Department to list terminations. Security Administration at the hosting Office or Department will lock the access privileges at the end of day on the effective date. This does not preclude the responsibility of all Offices and Departments to notify the hosting Office or Department of terminations using agreed upon formal notice or by the phone and/or email in the case of dismissals.
   (D) The Owning Office or Department will run a weekly report of transfers and follow up with the Office or Department concerned if a change notification is not received.
   (E) Users not using the system for 60 days will be automatically deactivated. Security Administration at the hosting Office or Department will notify the respective user's Office or Department and will require an email or new

activation form from the Office or Department's Security Representative to reactivate the individual.

(F) The hosting Office or Department has the responsibility to adhere to procedures and put into effect all authorized changes received from the owning County Office or Department in a timely manner.

2.4 INFORMATION SECURITY

1. The Office or Department that collects and maintains (owns) the information is responsible for interpreting all confidentiality restrictions imposed by laws and statutes as well as establishing information classification and approving information access. The hosting County Office or Department will staff a Security Administration function whose responsibility will be operational control and timely implementation of access privileges.

2. The Offices and Departments that access the systems have the responsibility to protect the confidentiality of information which they use in the course of their assigned duties.

2.5 INFORMATION AVAILABILITY

1. Information availability is the responsibility of the hosting Office or Department. Access to information will be granted as needed to all Offices and Departments to support their required processes, functions and timelines. Proven backup and recovery procedures for all information elements to cover the possible loss or corruption of system data are the responsibility of the hosting County Office or Department.

2. Required availability will vary with normal cycles of use (i.e. information is used constantly throughout the day but is only periodically accessed during the evening by a backup process, becomes archival after the backup is complete). The following asset availability definitions should include a statement detailing over what time period the definition is accurate for (i.e. Constant during business hours, archival after year-end, etc.):

Availability	Frequency of Use	Loss / Absence Impact
Regular	Constantly accessed at all times	Immediate cessation of supported business functions
Periodic	Accessed intermittently	Delay of supported business (i.e., year-end functions)
Archival	Not normally accessible	Disruption of business support objectives

3. The hosting Office or Department will be responsible for:

   (A) publishing a Service Level Agreement (SLA) for all users of the system including response time, hours of availability and all other services contracted,
   (B) ensuring all backups are current, secure and accessible,
   (C) ensuring information facilities and data can be recovered, and
   (D) ensuring adequate technical support for systems, database access and operating systems.

3.0 SECURITY PROGRAM MANAGEMENT

1. Managing information security within the County can be layered into three components:
2. MIS is responsible for direction and leadership in all aspects of information security.
3. County Offices and Departments that host data services are responsible for creating system specific policies and guidelines *to complement, but not contradict* those issued by MIS.
4. All County Offices and Departments are required to develop procedures specific to their information and process flows to protect the integrity of information and guard against misuse or loss. This is not limited to, but includes computer based information systems.

3.1 CENTRAL SECURITY PROGRAM

1. In regard to information services, MIS will develop, maintain and communicate polices and guidelines for the protection of information assets including but not

limited to hardware, software, information and communications. The Policy, Procedures, Guidelines and Best Practices will be mandatory for all Offices and Departments and represent the minimum standards that all Offices and Departments will adopt.

2. Minimum standards will be issued for:
   (A) systems planning,
   (B) systems development methodology,
   (C) documentation,
   (D) hardware requirements and compatibility,
   (E) operating systems compatibility,
   (F) software and hardware acquisition,
   (G) information security and internal controls,
   (H) database compatibility, and
   (I) contingency planning and disaster recovery.

3.2 HOSTING OFFICE AND DEPARTMENT SECURITY

1. Under the boundaries established by the minimum mandatory standards issued by MIS, Offices and Departments hosting information and systems for their own use or for the use of other Offices and Departments will further develop, maintain and communicate polices and guidelines for the protection of information assets including but not limited to hardware, software, information and communications.

2. All hosting Offices and Departments will:
   (A) follow a systems development methodology,
   (B) create and maintain adequate documentation,
   (C) develop hardware requirements and compatibility for review,
   (D) ensure operating systems compatibility,
   (E) expand and apply information security and internal controls,
   (F) ensure database compatibility, and
   (G) develop and test contingency planning and disaster recovery.

3.3 OFFICE AND DEPARTMENT SECURITY

1. All Offices and Departments have the responsibility of protecting their information assets from disclosure, loss or misuse. As such all Offices and Departments are required to adhere to and have documented procedures for:

   (A) security of information flow within their area of control,
   (B) information retention,
   (C) information disposal (including shredding and deletion of electronic information), and
   (D) communication of information security Policy, procedures, guidelines and best practices monitoring adherence with polices.

3.4 INCIDENT MANAGEMENT

1. Incident management responsibilities and procedures must be established by the hosting Office or Department to ensure a quick, effective and orderly response to security incidents. Procedures must be established to cover all potential types of security incidents, including:
   (A) information system failures and loss of service,
   (B) denial of service,
   (C) errors resulting from incomplete or inaccurate business information, and
   (D) breaches of confidentiality.

2. In addition to normal contingency plans (designed to recover systems or services as quickly as possible), the procedures must also cover:
   (A) analysis and identification of the cause of the incident,
   (B) planning and implementation of remedies to prevent recurrence, if necessary,
   (C) collection of audit trails and similar evidence,
   (D) communication with those affected by or involved with recovery from the incident, and
   (E) reporting the action to the security administration function at the hosting agency.

3. Audit trails and similar evidence must be collected and secured as appropriate, for:
   (A) internal problem analysis,
   (B) use as evidence in relation to a potential breach of contracts, policies, or regulatory requirements,

(C) use in the event of civil or criminal proceedings, e.g. under computer misuse or information protection, and
(D) use in negotiating for compensation from software and service suppliers.

4. Action to recover from security breaches and correct system failures should be carefully and formally controlled. The procedures must ensure that:
   (A) only clearly identified and authorized staff are allowed access to live systems and information,
   (B) all emergency actions taken are documented in detail,
   (C) emergency action is reported to management and reviewed in an orderly manner, and
   (D) the integrity of business systems and controls is confirmed with minimal delay.

3.5 EVENT LOGGING AND MONITORING

1. Audit logs recording exceptions and other security-relevant events must be produced and kept for an agreed period to assist in future investigations and access control monitoring. Audit logs should include:
   (A) user IDs,
   (B) dates and times for log-on and log-off,
   (C) terminal identity or location if possible,
   (D) records of successful and rejected system access attempts, and
   (E) records of successful and rejected data and other resource access attempts.

2. Certain audit logs may be required to be archived as part of the record retention procedures or because of requirements to collect evidence.

3. Procedures for monitoring use of information processing facilities must be established and the result of the monitoring activities reviewed regularly. Such procedures are necessary to ensure that users are only performing activities that have been explicitly authorized. The level of monitoring required for individual facilities should be determined by a risk assessment. Areas that should be considered include:

(A) Authorized access, including detail such as:
  (i) the user ID,
  (ii) the date and time of key events,
  (iii) the types of events,
  (iv) the files accessed, and
  (v) the program/utilities used.

(B) All privileged operations, such as:
  (i) use of supervisor account,
  (ii) system start-up and stop, and
  (iii) I/O device attachment/detachment.

(C) Unauthorized access attempts, such as:
  (i) failed attempts,
  (ii) access procedure violations and notifications for network gateways and firewalls, and
  (iii) alerts from proprietary intrusion detection systems.

(D) System alerts or failures such as:
  (i) console alerts or messages,
  (ii) system log exceptions, and
  (iii) network management alarms.

4.0 RISK MANAGEMENT

1. Risk management encompasses risk assessment, risk mitigation as well as evaluation and assessment. The risk assessment process includes identification and evaluation of risks and risk impacts and recommendation of risk-reducing measures. Risk mitigation refers to prioritizing, implementing and maintaining the appropriate risk-reducing measures recommended from the risk assessment process. Through a continual evaluation process, the hosting Office or Department is responsible for determining whether the remaining risk is at an acceptable level or whether additional security controls should be implemented to further reduce or eliminate the residual risk.

4.1 RISK ASSESSMENT

1. The hosting Office or Department will be responsible for determining the <u>likelihood</u> of an adverse event, the <u>threats</u> to system resources, the <u>vulnerability</u> of the system and the <u>impact</u> such an adverse event may have.

2. To determine the <u>likelihood</u> of an adverse event, consider:
   (A) Motivation

(B) Nature of the vulnerability
(C) Current controls

3. A threat needs, and cannot exist without a vulnerability. A vulnerability is a weakness that can be intentionally or accidentally triggered. Threats can be posed from a lot of sources, some of which are:
   (A) System Intruders (hackers)
   (B) Criminals
   (C) Terrorists
   (D) Espionage
   (E) Insiders which could be malicious or a result of poor training

4. In identifying the vulnerabilities, consideration must be given to:
   (A) Hardware
   (B) Software
   (C) Network
   (D) System Interfaces
   (E) Data and information
   (F) People who support and use the system
   (G) Information sensitivity

5. The impact of an adverse event is the:
   (A) Loss of Integrity
   (B) Loss of Availability
   (C) Loss of Confidentiality

4.2 RISK MITIGATION

1. All hosting Offices and Departments are responsible for reducing risk to all information assets. The following are options provided in analyzing the alternatives.
   (A) Risk Assumption. To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level.
   (B) Risk Avoidance. To avoid the risk by eliminating the risk cause and/or

consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified).

(C) Risk Limitation. To limit the risk by implementing controls that minimizes the adverse impact of a threat exercising a vulnerability (e.g., use of supporting, preventive, detective controls).

(D) Risk Planning. To manage risk by developing a risk mitigation plan that prioritizes, implements and maintains controls.

(E) Research and Acknowledgment. To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability.

(F) Risk Transference. To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

5.0 PERSONNEL/USER ISSUES

1. Personnel awareness of the Information Security Policy, procedures, guidelines and best practices is the responsibility of all Offices and Departments. Adherence to the Policy, procedures, guidelines and best practices is the responsibility of all County Offices and Departments on behalf of their employees.

2. Information security must be adopted at all levels as a "norm" of job performance. Information systems and data are vulnerable. With constant re-enforcement and monitoring, individuals will accept their responsibility to protect the information assets of the County and relate their performance in this area to standards of performance.

3. The IT staff must be alert and trained in offensive and defensive methods to protect the County's information assets. Adequate staffing and key position backup are essential to run and maintain a secure environment.

5.1 STAFFING

1. Adequate staffing, training and backup are the responsibility of all hosting Offices and Departments. Each Office and Department will be responsible for:
   (A) ensuring qualifications meet position requirements,
   (B) identifying roles that will impact operations when not filled, i.e. if the incumbent leaves or cannot perform the function,

(C) ensuring training is in place to keep key individuals current with the technology available in the marketplace (this is particularly important with regards to the Internet and database controls), and
(D) documenting contingency plans if critical functions are not available.

5.2 AWARENESS/TRAINING

1. Awareness is not training. The purpose of awareness presentations are simply to focus attention on security and are intended to allow individuals to recognize IT security concerns and respond accordingly. Awareness relies on reaching broad audiences, whereas training is more formal, having a goal of building knowledge and skills to facilitate job performance.

2. Effective IT security awareness presentations must be designed. Awareness presentations must be on-going, creative and motivational, with the objective of focusing attention so that the learning will be incorporated into conscious decision making.

3. MIS will be responsible for:
   (A) Communicating the minimum standards for all related policies and procedures,
   (B) Providing recommendations for best practices in selected areas related to information security, and
   (C) Providing all necessary information for the development of an awareness program by County Offices and Departments

4. All County Offices and Departments will:
   (A) create and present security awareness sessions for their staff members, and
   (B) ensure all staff members have attended an awareness session.

5. All current employees as well as new employees or contractors when hired that have access to any information assets must be briefed by the hiring or contracting Office or Department as follows:
   (A) the access requirements of their position or contract,

(B) their responsibilities for safeguarding sensitive information and assets,
(C) all information security policies, procedures, guidelines and best practices, and
(D) a written document outlining the contents of the briefing and the date, which should be signed by the individual briefed acknowledging receipt of its contents.

5.3 PERSONAL COMPUTER USAGE

1. The computers of the County are provided for job related activities. To this end, the hosting Office or Department provides support in networking and information resources for its computing community.

2. All users are given access to computers for job related duties and this usage must remain in compliance with County, Office and/or Departmental policies as well as all state and federal laws governing usage and communication of information. Failure to comply will result in the denial of access privileges and may for employees lead to disciplinary action up to and including dismissal. For contractors, it may lead to the cancellation of the contractual agreement. Litigation may ensue.

3. In the effort to protect the integrity of the County network and its systems, any proof of unauthorized or illegal use of any County computer and/or its accounts will warrant the immediate loss of access to these files, accounts and/or systems by the hosting Office or Department security and information systems staff and appropriate action will be taken.

4. Information Security Policy for computer usage prohibits the use of its resources to:
   (A) Send email using someone else's identity (Email forgery).
   (B) Take any action that knowingly will interfere with the normal operation of the network, its systems, peripherals and/or access to external networks.
   (C) Install any system or software on the network without prior approval.
   (D) Install any software systems or hardware that will knowingly install a virus, Trojan horse, worm or any other known or unknown destructive mechanism.
   (E) Attempt IP spoofing.
   (F) Attempt the unauthorized downloading, posting or dissemination of copyrighted materials.
   (G) Attempt any unauthorized downloading of software from the Internet.

(H) Transmit personal comments or statements in a manner that may be mistaken as the position of the County.

(I) Access, create, transmit (send or receive), print or download material that is discriminatory, derogatory, defamatory, obscene, sexually explicit, offensive or harassing based on gender, race, religion, national origin, ancestry, age, disability, medical condition, sexual orientation or any other status protected by state and federal laws.

5. Furthermore, it is the County's position that all messages sent and received, including personal messages and all information stored on the County's electronic mail system, voicemail system or computer systems are County property regardless of the content. As such, the hosting Office or Department reserves the right to access, inspect and monitor the usage of all its technology resources including any files or messages stored on those resources at any time, in its sole discretion, in order to determine compliance with its policies, for purposes of legal proceedings, to investigate misconduct, to locate information or for any other business purpose.

5.4 EMAIL USAGE

1. Electronic mail (email) is a highly efficient form of modern communication media. Used appropriately, email provides people with a means to communicate thereby facilitating business contact. However, this convenience also tempts users to experiment or take advantage of this media, resulting in email of unwelcome types (collectively known along with other unwelcome activity as Net Abuse). The improper use of this email technology may jeopardize systems integrity, security and service levels. Access to email is provided to users to assist them to perform their work and their use of email must not jeopardize operation of the system or the reputation and/or integrity of the County.

2. Email accounts are made available to all Office and Department staff that require the service for the performance of job-related functions. The following statements apply:

(A) All email, and associated system resources are the property of the County. Email is subject to the same restrictions on its use and the same review process as is any other government furnished resource provided for the use of employees. Its use and content may be monitored.

(B) Email usage must be able to withstand public scrutiny. Users must comply with all applicable legislation, regulations, policies and standards. This includes complying with copyright and license provisions with respect to both programs and data.

(C) While email is provided as a business tool to users, its reasonable, incidental use for personal purposes is acceptable. This use must not, however, detrimentally affect employee productivity, disrupt the system and/or harm the government's reputation.

3. Users may not:
   (A) use email for commercial solicitation or for conducting or pursuing their own business interests or those of another organization,
   (B) use email to distribute hoaxes, chain letters or advertisements and/or send rude, obscene, threatening or harassing messages,
   (C) use email to distribute pornographic material or hate literature,
   (D) use email to harass other staff members,
   (E) use email to send executable programs or games,
   (F) use email to send potentially offensive material, and
   (G) propagate viruses knowingly or maliciously.
4. Users must not send, forward and/or reply to large distribution lists concerning non-government business. In addition, users must consider the impact on the network when creating and using large, work-related distribution lists.
5. Email is a record and therefore management of email must comply with existing legislation, regulations, policies and standards.
6. Alleged inappropriate use of the email technology will be reviewed by the Office or Department involved as well as the hosting Office or Department on a case-by-case basis and may lead to disciplinary action up to and including dismissal. In respect to contractors, it may lead to cancellation of the contractual arrangement. In any of the cases, it may lead to litigation.

5.5 INTERNET/INTRANET SECURITY

1. The World Wide Web (WWW) is a system for exchanging information over the Internet. An Intranet is a proprietary network that is specific for an entity, such as the County.

2. At the most basic level, the Web can be divided in two principal components: Web servers, which are applications that make information available over the Internet (in essence publish information) and Web browsers (clients), which are used to access and display the information stored on the Web servers. The Web server is the most targeted and attacked host on most organizations' network. As a result, it is essential to secure Web servers and the network infrastructure that supports them.

3. The specific security threats to Web servers generally fall into one of the following categories:
   (A) Malicious entities may exploit software bugs in the Web server, underlying operating system or active content to gain unauthorized access to the Web server. Examples of unauthorized access are gaining access to files or folders that were not meant to be publicly accessible or executing privileged commands and/or installing software on the Web server.
   (B) Denial of Service attacks may be directed to the Web server denying valid users an ability to use the Web server for the duration of the attack.
   (C) Sensitive information on the Web server may be distributed to unauthorized individuals.
   (D) Sensitive information that is not encrypted when transmitted between the Web server and the browser may be intercepted.
   (E) Information on the Web server may be changed for malicious purposes. Web site defacement is a commonly reported example of this threat.
   (F) Malicious entities may gain unauthorized access to resources elsewhere in the organization's computer network via a successful attack on the Web server.
   (G) Malicious entities may attack external organizations from a compromised Web server, concealing their actual identities and perhaps making the organization from which the attack was launched liable for damages.
   (H) The server may be used as a distribution point for illegal copies software attack tools, or pornography, perhaps making the organization liable for damages.

4. The hosting Office or Department is responsible for the Web server. Some examples of controls to protect from unauthorized access or modification are:

(A) install or enable only necessary services,
(B) install Web content on a dedicated hard drive or logical partition,
(C) limit uploads to directories that are not readable by the Web server,
(D) define a single directory for all external scripts or programs executed as part of Web content,
(E) disable the use of hard or symbolic links,
(F) define a complete Web content access matrix that identifies which folders and files within the Web server document directory are restricted and which are accessible (and by whom), and
(G) use host-based intrusion detection systems and/or file integrity checkers to detect intrusions and verify Web content.

5. Maintaining a secure Web server is the responsibility of the hosting Office or Department and involves the following steps:
   (A) configuring, protecting and analyzing log files,
   (B) backing up critical information frequently,
   (C) maintaining a protected authoritative copy of the organization's Web content,
   (D) establishing and following procedures for recovering from compromise,
   (E) testing and applying patches in a timely manner, and
   (F) testing security periodically.

6. A firewall environment must be employed to perform the following general functions:
   (A) filter packets and protocols,
   (B) perform inspection of connections,
   (C) perform proxy operations or selected applications,
   (D) monitor traffic allowed or denied by the firewall, and
   (E) provide authentication to users using a form of authentication that does not rely on static, reusable passwords that can be sniffed.

7. The hosting Office or Department responsible for Internet security will:
   (A) Keep operational systems and applications software up to date. Because software systems are so complex, it is common for security related problems to be discovered only after the software has been in widespread use. Although most vendors try to address known security flaws in a timely manner, there is normally a gap from the time the problem is publicly known, the time the vendor requires to prepare corrections and the time you install the update. This gap gives potential intruders an opportunity to take advantage of this flow and mount an attack on

computers and networks. To keep this time interval as short as possible, it is required to stay aware of:

(i) announcements of security-related problems that may apply,
(ii) immediate actions to reduce exposure to the vulnerability, such as disabling the affected software and
(iii) permanent fixes from vendors.

(B) Restrict only essential network services and operating system on the host server.
    (i) Ensure that only the required set of services and applications are installed on the host server. Either do not install unnecessary services or turn the services off and remove the corresponding files (and any other unnecessary files) from the host.
(C) Configure computers for file backup.
(D) Protect computers from viruses and programmed threats.
(E) Allow only appropriate physical access to computers.
(F) Design, implement and monitor an effective firewall system.

6.0 HELP DESK MANAGEMENT

1. A world class Help Desk is characterized by responsiveness, knowledge, feedback and improvement. The speed at which issues are resolved, the number of requests handled by the first level in support, the follow-up with the user community on status, security and the monitoring of performance with the goal of continuous improvement are the characteristics that separate a progressive, secure, mission critical operation from the ordinary, reactive operation.

2. The mandate of the help desk function should include:
   (A) Adherence to all policies and procedures as published.
   (B) Recommendation of new and/or changes to policies and procedures.
   (C) Ownership of all the calls until reassigned or routed.
   (D) Performance of all front-line tasks such as password resets, printer resets, etc.
   (E) Routing of system or technical queries to the knowledge expert responsible.
   (F) Reporting on and monitor calls.
   (G) Reporting and escalation of all incidents of suspicious activity or violations of security.

3. The following is a list of suggested reports required for managing the Help Desk.

   (A) Incident Report - Content: all known information, status. Schedule: Immediately. Distribution: Security Administration at hosting Office or Department.
   (B) Call Activity - Content: calls by type, Office or Department, severity average resolution time. Schedule: Monthly. Distribution: Management.
   (C) Open Calls - Content: calls by user agency, severity, ranked by oldest time open. Schedule: Weekly. Distribution: Help Desk, Knowledge Experts.
   (D) Daily Activity - Content: calls received by time of day. Schedule: Daily. Distribution: Help Desk.
   (E) Repeat Calls - Content: number of calls ranked by user (over 3) showing Agency, type. Schedule: Monthly. Distribution: Knowledge Expert and Director of the agency generating the calls.

6.1 SUPPORT CALLS

1. Call handling and routing is the responsibility of the hosting Office's or Department's help desk function. This function should present a standard front to all users of their services including telephone calls, emails and voice mails. Information on all calls will be logged and violations in security or suspicious activity will be reported immediately to the appropriate designated authority. The help desk function will verify the identity of the caller by:
   (A) Obtaining their name.
   (B) Requesting additional information, such as:
      (i) User ID *(interchangeable with Log-on ID)*
      (ii) Office or Department
      (iii) Phone number

6.2 PASSWORD RESETS

1. Password resets are the responsibility of the hosting County Office or Department's help desk function. Identities of requestors will be verified by the help desk, logged and confirmed back to the user at the respective County Office or Department.

2. It is the responsibility of the requestor from all County Offices and Departments, in requesting a password reset, to confirm their identity. This may be accomplished by:
   (A) Providing their name.
   (B) Answering a unique question and answer submitted on sign up, such as: place of birth, mother's maiden name, etc.).
   (C) Providing additional information as may be requested, such as:
      - Office or Department
      - Phone number

3. The responsibility of the host Office or Department's Help Desk is to:
   (A) Confirm the identity of the requestor.
   (B) Report all suspicious activity to the Security Administrator immediately. Discrepancies in answers, inability to provide the correct User ID, frequent

requests for changes to the same User ID, or obvious password sharing constitute security breaches and will be reported.

(C) Reset the password.
(D) Log details of the call.
(E) Confirm the password reset to the user registered to the User ID via email.
(F) Report activity monthly to each County Office or Department involved.

6.3 VOICE MAIL SECURITY

1. The voice mail feature of many PBXs can be a particularly vulnerable feature. This is because voice mail is typically used to let someone store voice messages at a central location by calling in from any inside or outside line and then retrieve the messages from any inside or outside line. It also grants the general public access to the PBX system.

2. In retrieving messages, the target extension and a password are usually required to gain access to the messages. Since the target extension is usually easy to determine, the only significant restriction to an adversary is the password. Once an adversary determines a target user's password all messages left for the target user are accessible to the adversary. The adversary could also delete messages from the target user's mailbox to prevent an important message from getting to the target user. Some guidelines to secure the contents of voice mail include the following:
   (A) Default and obvious passwords must be changed at initial log-in. The target user's extension is easily known. Default passwords established at system initialization time may never have been changed. Fixed length passwords are more vulnerable than variable length passwords.
   (B) Non-terminated password entry should be avoided. Some systems accept a continuous string of digits, granting entry when the correct password sequence is entered. By not requiring a password entry to be terminated, the length of the average sequence needed to guess a four digit password is reduced by a factor of five.
   (C) A complete password must be entered before an incorrect password is rejected. If it is rejected on the first incorrect digit, sequential guessing becomes much more practical. For example, on such a system that has a fixed password length of four and uses the digits 0-9, it would take at most 40 sequential attempts to guess a password. On a system that required all four digits to be entered at most 10,000 guesses would be required.
   (D) Disallow access to external lines via the Voice Mail system.

7.0 PHYSICAL AND ENVIRONMENTAL SECURITY

1. The hosting Office or Department has the responsibility for documentation, execution, monitoring and testing of a physical security plan for both computer and telecommunication assets. This physical security plan would evaluate the risks from potential losses due to:
   (A) physical destruction or theft of physical assets,
   (B) loss or destruction of information and program files,
   (C) theft of information,
   (D) theft of indirect assets, and
   (E) delay or prevention of computer processing.

2. Included in the plan would be measures for reducing the possibility of a loss and must address:
   (A) changes in the environment to reduce exposure,
   (B) measures to reduce the effect of a threat,
   (C) improved control procedures,
   (D) early detection, and
   (E) contingency plans.

7.1 OPERATIONS CENTER

1. The following are guidelines of the action items for establishing, implementing and maintaining a physical security program at the hosting Office or Department:
   (A) conduct a risk analysis,
   (B) determine local natural disaster probabilities,
   (C) protect supporting utilities
   (D) ensure computer reliability,
   (E) provide physical protection
   (F) implement procedural security,
   (G) plan for contingencies,
   (H) develop security awareness, and
   (I) validate the program.

7.2 OPERATIONS MONITORING

1. Hosting Offices or Departments can monitor security effectiveness by comparing performance to the metrics in a SLA and incidents that occur in violation of security policies, procedures, guidelines and best practices.

2. Guidelines for hosting Offices or Departments in establishing a SLA are:
   (A) hours of system availability,
   (B) hours of application system support,
   (C) hours of technical support,
   (D) off hours support,
   (E) average system response time, and
   (F) other metrics as suitable for agency specific applications.
3. Hosting agencies should have a goal of achieving 99.9%+ of the metrics established in the service level agreement. Failure to achieve these targets could be an indication of security breaches.

4. Insofar as incidents are concerned, both offensive and defensive actions to protect the security of physical assets should be considered routine. Examples of offensive actions include:
   (A) routine changes of passwords,
   (B) develop an escalation procedure of incidents,
   (C) routine changes of locks or combinations to the facilities,
   (D) have more than one person knowledgeable for critical functions,
   (E) rotate shifts or people between functions,
   (F) monitor all incursion attempts,
   (G) install latest versions of firewall software,
   (H) maintain 24x7 vendor contact list,
   (I) routine backups,
   (J) off-site storage of system information and programs,
   (K) redundant components and lines for critical systems, and
   (L) testing of recovery procedures.

5. Examples of defensive actions include:
   (A) report and action all deviations to security policies, procedures, guidelines and best practices,
   (B) shut down any infected machine immediately,
   (C) disconnect any problem areas from the network,
   (D) revoke privileges of users violating policies,

(E) assign severity to an issue and escalate, and
(F) acquire knowledgeable resources.

7.3 BACK-UP OF INFORMATION

1. Back-up copies of essential business information and software must be taken regularly. Adequate backup facilities should be provided to ensure that all essential business information and software can be recovered following a disaster or media failure. Backup arrangements for individual systems should be regularly tested to ensure that they meet the requirements of business continuity plans. The following controls must be considered:
   (A) A minimum level of back-up information, together with accurate and complete records of the back-up copies and documented restoration procedures, should be stored in a remote location at a sufficient distance to escape any damage from a disaster at the main site. At least three generations or cycles of back-up information should be retained for important business applications.
   (B) Back-up information should be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site. The controls applied to media at the main site should be extended to cover the back-up site.
   (C) Back-up media should be regularly tested, where practicable, to ensure that they can be relied upon for emergency use when necessary.
   (D) Restoration procedures should be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.
   (E) The retention period for essential business information and any requirement for archive copies to be permanently retained should be determined.

7.4 ACCESS CONTROL

1. Logical and physical access controls are required to ensure the integrity of the information and physical assets.

2. The following guidelines for controlling logical access should be implemented by all hosting Offices and Departments:
   (A) document and adhere to procedures for granting, modifying and revoking access,
   (B) ensure segregation of duties for access
   (C) install detection mechanisms for unauthorized access attempts,
   (D) timeout a session after 15 minutes of inactivity, and
   (E) revoke access after an inactivity period of 60 days.

3. Physical access control guidelines for all agencies include:
   (A) all telecommunication and computer related equipment are to be in a secured, locked environment,
   (B) access codes for secure environments must be changed at least every 60 days or in the event of an individual departing that previously had access,
   (C) account for all keys issued for those facilities using this method and replace locking mechanism when a key is missing,
   (D) when the system permits, log all access and retain, and
   (E) secure all peripherals such as air conditioning, generators, etc.
   (F) segregation of duties must be implemented to prevent unauthorized access to systems or data

7.5 NETWORK

1. Unsecured connections to network services can affect the whole organization. Users must only have direct access to the services that they have been specifically authorized to use. This control is particularly important for network connections to sensitive or critical business applications or to users in high-risk locations, e.g. public or external areas that are outside the organization's security management and control.
2. Procedures concerning the use of networks and network services should cover:
   (A) the networks and network services which are allowed to be accessed,
   (B) authorization procedures for determining who is allowed to access which networks and networked services, and
   (C) management controls and procedures to protect the access to network connections and network services.

3. The path from the user terminal to the computer service must be controlled. Networks are designed to allow maximum scope for a sharing of resources and flexibility of routing. These features may also provide opportunities for unauthorized access to business applications, or unauthorized use of

information facilities. Incorporating controls that restrict the route between a user terminal and the computer services its user is authorized to access, e.g. creating an enforced path can reduce such risks. The objective of an enforced path is to prevent any users selecting routes outside the route between the user terminal and the services that the user is authorized to access. This usually requires the implementation of several controls at different points in the route. The principle is to limit the routing options at each point in the network, through predefined choices.

4. The following methods should be implemented to limit the path to a service:
   (A) allocating dedicated lines or telephone numbers,
   (B) automatically connecting ports to specified application systems or security gateways,
   (C) limiting menu and submenu options for individual users,
   (D) preventing unlimited network roaming,
   (E) enforcing the use of specified application systems and/or security gateways for external network users,
   (F) actively controlling allowed source to destination communications via security gateways, e.g. firewalls, and
   (G) restricting network access by setting up separate logical domains, e.g. virtual private networks, for user groups within the organization.

5. External connections provide a potential for unauthorized access to business information, e.g. access by dial-up methods. Therefore, access by remote users must be subject to authentication. There are different types of authentication methods, some of these provide a greater level of protection than others, e.g. methods based on the use of cryptographic techniques can provide strong authentication. It is important to determine from a risk assessment the level of protection required. This is needed for the appropriate selection of an authentication method.
   (A) Authentication of remote users should be achieved using one of the following techniques:
   (B) a cryptographic based technique,
   (C) hardware tokens,
   (D) a challenge/response protocol,

(E) dedicated private lines or a network user address checking, and
(F) call-back procedures.

6. Dial-back procedures and controls, e.g. using dial-back modems, can provide protection against unauthorized and unwanted connections to an organization's information processing facilities. This type of control authenticates users trying to establish a connection to an organization's network from remote locations. When using this control an organization should not use network services which include call forwarding or, if they do, they should disable the use of such features to avoid weaknesses associated with call forwarding. It is also important that the call back process includes ensuring that an actual disconnection on the organization's side occurs. Otherwise, the remote user could hold the line open pretending that call back verification has occurred. Call back procedures and controls should be thoroughly tested for this possibility.

7. A facility for automatic connection to a remote computer could provide a way of gaining unauthorized access to a business application. Connections to remote computer systems must therefore be authenticated. This is especially important if the connection uses a network that is outside the control of the organization's security management. Node authentication can serve as an alternative means of authenticating groups of remote users where they are connected to a secure, shared computer facility.

8. Access to diagnostic ports must be securely controlled. Many computers and communication systems are installed with a dial-up remote diagnostic facility for use by maintenance engineers. If unprotected, these diagnostic ports provide a means of unauthorized access. They should therefore be protected by an appropriate security mechanism, e.g. a key lock and a procedure to ensure that they are only accessible by authorized people.

9. Networks are increasingly being extended beyond traditional organizational boundaries as business partnerships are formed that may require the interconnection or sharing of information processing and networking facilities. Such extensions will increase the risk of unauthorized access to already existing information systems that use the network, some of which might require protection from other network users because of their sensitivity or criticality. In such circumstances, controls must be introduced in networks to segregate groups of information services, users and information systems.

10. The security of large networks should be controlled by dividing them into separate logical network domains, e.g. an organization's internal network domains and external network domains, each protected by a defined security perimeter. Such a perimeter should be implemented by installing a secure gateway between the two networks to be interconnected to control access and information flow between the two domains. This gateway should be configured to filter traffic between these domains and to block unauthorized access in accordance with the organization's access control procedures. An example of this type of gateway is what is commonly referred to as a firewall. The criteria for segregation of networks into domains should be based on the access control procedures and access requirements and also take account of the relative cost and performance impact of incorporating suitable network routing or gateway technology.

11. The connection capability of users must be restricted in shared networks, in accordance with the access control procedures.

12. Such controls should be implemented through network gateways that filter traffic by means of pre-defined tables or rules. The restrictions applied should be based on the access procedures and requirements of the business applications and should be maintained and updated accordingly. Examples of applications to which restrictions should be applied are:
    (A) electronic mail,
    (B) one-way file transfer,
    (C) both-ways file transfer,
    (D) interactive access, and
    (E) network access linked to time of day or date.

13. Shared networks must have routing controls to ensure that computer connections and information flows do not breach the access control procedures of business applications. This control is essential for networks shared with third party (nonorganizational) users.

14. Routing controls should be based on positive source and destination address checking mechanisms. Network address translation is also a very useful

mechanism for isolating networks and preventing routes to propagate from the network of one organization into the network of another. They can be implemented in software or hardware. Implementers should be aware of the strength of any mechanisms deployed. A wide range of public or private network services is available, some of which offer value added services. Network services may have unique or complex security characteristics.

15. A clear description of the security attributes of all network services used by the organization must be provided.

7.6 ELECTRONIC COMMERCE SECURITY

1. Electronic commerce can involve the use of electronic data interchange (EDI), electronic mail and online transactions across public networks such as the Internet. Electronic commerce is vulnerable to several network threats which may result in fraudulent activity, contract dispute and disclosure or modification of information and must be protected. The following issues must be resolved:

   (A) Authentication. What level of confidence should the customer and trader require in each other's claimed identity?
   (B) Authorization. Who is authorized to set prices, issue or sign key trading documents? How does the trading partner know this?
   (C) Contract and tendering processes. What are the requirements for confidentiality, integrity and proof of dispatch and receipt of key documents and the non-repudiation of contracts?
   (D) Pricing information. What level of trust can be put in the integrity of the advertised price list and the confidentiality of sensitive discount arrangements?
   (E) Order transactions. How is the confidentiality and integrity of order, payment and delivery address details and confirmation of receipt, provided?
   (F) Vetting. What degree of vetting is appropriate to check payment information supplied by the customer?
   (G) Settlement. What is the most appropriate form of payment to guard against fraud?
   (H) Ordering. What protection is required to maintain the confidentiality and integrity of order information and to avoid the loss or duplication of transactions?
   (I) Liability. Who carries the risk for any fraudulent transactions?

2. Electronic commerce arrangements between trading partners should be supported by a documented agreement which commits both parties to the

agreed terms of trading, including details of authorization. Other agreements with information service and value-added network providers may be necessary.

3. Consideration should be given to the resilience to attack of the host used for electronic commerce and the security implications of any network interconnection required for its implementation.

7.7 MOBILE COMPUTING

1. Formal procedures must be in place and appropriate controls must be adopted to protect against the risks of working with mobile computing facilities, in particular in unprotected environments. For example, such procedures should include the requirements for:
   (A) physical protection,
   (B) access controls,
   (C) cryptographic techniques,
   (D) back-ups, and
   (E) virus protection.

2. Procedures should also include rules and advice on connecting mobile facilities to networks and guidance on the use of these facilities in public places.

3. Care should be taken when using mobile computing facilities in public places, meeting rooms and other unprotected areas outside of the organization's premises. Protection should be in place to avoid the unauthorized access to or disclosure of the information stored and processed by these facilities, e.g. using cryptographic techniques.

4. It is important that when such facilities are used in public places care is taken to avoid the risk of overlooking by unauthorized persons. Procedures against malicious software should be in place and be kept up to date. Equipment should be available to enable the quick and easy back-up of information. These back-ups should be given adequate protection against, e.g., theft or loss of information.

5. Suitable protection should be given to the use of mobile facilities connected to networks.

6. Remote access to business information across public network using mobile computing facilities should only take place after successful identification and authentication and with suitable access control mechanisms in place.

7. Mobile computing facilities should also be physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centers and meeting places. Equipment carrying important, sensitive and/or critical business information should not be left unattended and, where possible, should be physically locked away, or special locks should be used to secure the equipment.

7.8 REMOTE COMPUTING

1. Remote computing uses communications technology to enable staff or agencies to work remotely from a fixed location outside of their organization. Suitable protection of the remote computing site should be in place against, e.g., the theft of equipment and information, the unauthorized disclosure of information, unauthorized remote access to the organization's internal systems or misuse of facilities. It is important that remote computing is both authorized and controlled by management and that suitable arrangements are in place for this way of working.

2. Procedures must be developed from best practices to authorize and control remote computing activities. Offices and Departments should only authorize remote computing activities if they are satisfied that appropriate security arrangements and controls are in place and that these comply with the Office's or Department's security procedures.
   The following should be considered:
   (A) the existing physical security of the remote computing site, considering the physical security of the building and the local environment,
   (B) the communications security requirements, considering the need for remote access to the organization's internal systems, the sensitivity of the information that will be accessed and passed over the communication link and the sensitivity of the internal system, and
   (C) the threat of unauthorized access to information or resources from other people using the accommodation.

3. The controls and arrangements to be considered include:
   (A) the provision of suitable equipment and storage furniture for the remote computing activities,
   (B) a definition of the work permitted, the hours of work, the classification of information that may be held and the internal systems and services that the user is authorized to access,
   (C) the provision of suitable communication equipment, including methods for securing remote access,
   (D) physical security,
   (E) the provision of hardware and software support and maintenance,
   (F) the procedures for back-up and business continuity, and
   (G) audit and security monitoring.

7.9 EXTERNAL FACILITIES

1. The use of an external contractor to manage information processing or communication facilities may introduce potential security exposures, such as the possibility of compromise, damage or loss of data at the contractor's site.

2. Prior to using external facilities, the risks must be identified, and appropriate controls agreed with the contractor and incorporated into the contract. Issues that should be addressed include:
   (A) identifying sensitive or critical applications better retained in-house,
   (B) obtaining the approval of business application owners,
   (C) implications for business continuity plans,
   (D) security standards to be specified and the process for measuring compliance,
   (E) allocation of specific responsibilities and procedures to effectively monitor all relevant security activities, and
   (F) responsibilities and procedures for reporting and handling security incidents.

7.10 ENCRYPTION

1. Encryption should be applied to protect the confidentiality of sensitive or critical information.

2. Based on a risk assessment, the required level of protection should be identified considering the type and quality of the encryption algorithm used and the length of cryptographic keys to be used.

3. Specialist advice should be sought to identify the appropriate level of protection, to select suitable products that will provide the required protection and the implementation of a secure system of key management. In addition, legal advice may need to be sought regarding the laws and regulations that might apply to the organization's intended use of encryption.

4. Procedures for the use of cryptographic controls for the protection of information must be developed and followed. Such procedures are necessary to maximize benefits and minimize the risks of using cryptographic techniques and to avoid inappropriate or incorrect use.

5. When developing procedures the following should be considered:
   (A) the management guidelines on the use of cryptographic controls across the organization,
   (B) including the general principles under which business information should be protected,
   (C) the approach to key management, including methods to deal with the recovery of encrypted information in the case of lost, compromised or damaged keys,
   (D) roles and responsibilities, e.g. who is responsible for: the implementation of the procedures; the key management,
   (E) how the appropriate level of cryptographic protection is to be determined, and
   (F) the standards to be adopted for the effective implementation throughout the organization (which solution is used for which business processes).

8.0 BUSINESS CONTINUITY

1. Information Technology facilities and systems are vulnerable to a variety of disruptions, some of which are short term (measured in minutes and hours) and others lasting for a day or longer. The intent of Business Continuity Planning is to be alert and ready to sustain an organization's processes during and following a significant unforeseen disruption in services caused by disasters and security failures.

2. Business continuity should begin by identifying events that can cause interruptions to business processes, e.g. equipment failure, flood and fire. This should be followed by a risk assessment to determine the impact of those interruptions (both in terms of magnitude and recovery time frame). Both activities should be carried out with full involvement from owners of business resources and processes. This assessment considers all business processes and is not limited to the information processing facilities.

3. A strategy plan, based on appropriate risk assessment, must be developed for the overall approach to business continuity.

4. All hosting County Offices and Departments will develop contingency plans for each major application or general support system to meet the needs of critical IT operations in the event of a disruption extending beyond a given time. The length of the time may vary with the system or facility involved. The procedures for execution of such a capability will be documented in a formal contingency plan, be reviewed annually and updated as necessary by the hosting Office or Department. The procedures must account for differential daily backups and complete weekly backups to be conducted and sent to a designated off-site facility. As well, the plans should assign specific responsibilities to designated staff or positions to facilitate the recovery and/or continuity of essential IT functions. Designated personnel will be trained to execute contingency procedures. An annual test of the recovery procedures will be conducted.

5. Business continuity management should include controls to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.

8.1 CONTINGENCY PLAN

1. A contingency plan provides the documented organizational plan to mitigate risks of business interruption and minimize the impact of any disruption of service. It must maintain instructions for achieving a full or minimally acceptable set of business objectives in the absence of assets, through cost-effective strategies to provide replacements for assets as they become unavailable. The Plan must involve advance planning and preparations to respond to external circumstances as determined by a risk assessment and continue to provide a pre-determined acceptable level of business functionality. Procedures and guidelines must be defined, implemented, tested and maintained to ensure continuity of organizational services in the event of a disruption. Each contingency plan is unique and must be tailored to organization's requirements; it must be flexible enough to allow additions, modifications and maintenance. The plan should minimize dependency on individuals for interpretation and implementation – in the event of emergency, key personnel may not be available. It must ensure completeness and establish critical decisions. Always make sure that the plan remains current. The following questions must be answered:

    (A) What risks the organization is facing in terms of their likelihood and their impact, including an identification and prioritization of critical business processes?
    (B) How long can the enterprise operate without this asset?
    (C) What are the impact interruptions are likely to have on the business (it is important that solutions are found that will handle smaller incidents, as well as serious incidents that could threaten the viability of the organization), and establishing the business objectives of information processing facilities?
    (D) What is the maximum acceptable delay before which temporary systems must be made available?
    (E) What is the minimum time in which temporary systems may be expected to become available?
    (F) At what minimally acceptable level of functionality can the enterprise operate?
    (G) How long can the enterprise operate at a minimally acceptable level of performance?
    (H) At what point can the enterprise begin to resume normal operations?
    (I) At what point must the enterprise begin to resume normal operations?

2. A Contingency Plan should contain the roles, responsibilities and procedures for restoring a system or facility following a major disruption. The following guidelines represent the stages to be followed in preparing and executing a Contingency Plan:
   (A) Documentation - A plan must be documented, tested and communicated. Included in the plan should be a mission, a scope of what is included and not included assumptions, requirements, staffing and responsibilities.
   (B) Notification/Activation - Internally within IT, the notification, timing and paths should be documented. There should only be one voice talking for the recovery team for communication and escalation outside the boundaries of IT. Immediately following damage assessment, the plan is activated.
   (C) Recovery - The sequence of recovery activities should be documented in procedures. These activities are to restore operations which may be in temporary locations or with incomplete data.
   (D) Reconstitution - Restoring facilities and systems to the "norm" will include testing and proof of operations viability.
   (E) What equipment / facilities are expected to be unavailable?
   (F) What is the timing of the disruption?
   (G) What records, files and materials may or may not be expected to be protected from destruction?
   (H) What resources are available or required following the event?
      (i) Applications / Processes
      (ii) Functionality / Capacity
      (iii) Equipment / Infrastructure
      (iv) Staff /Skills
      (v) Connectivity / Network
      (vi) Data Sources
      (vii) Facilities / Services / Physical Premises
      (viii) Transportation
      (ix) Documentation / Reference material
      (x) Security Policies and Procedures
      (xi) Specific Policies and Procedures
      (xii) Authorization

3. Following is a list of considerations that, at a minimum, must be addressed in creating contingency plans:
   (A) What additional security measures are required to protect assets in the planning, execution and maintenance of procedures to assure business continuity?
   (B) What degree of functionality is still available at the main facility, if any?
   (C) Availability of staff to perform critical functions defined within the plan.
   (D) Ability of staff to be notified and report to the backup site(s) to execute contingency plans.
   (E) Backup files and recovery methods.
   (F) Off-site storage facilities and materials availability.
   (G) Disaster recovery plan.
   (H) Suitability of subsets of the overall plan, to be used to recover from minor interruptions.
   (I) Availability of an alternate facility.
   (J) Off-site availability of critical forms and supplies, either at an alternate facility or off-site storage.
   (K) Existence of a backup site for processing the organization's work.
   (L) Availability of long distance and local communications lines.
   (M) Quality of surface transportation in from local to remote sites.
   (N) Ability of vendors to perform according to their general commitments to support the organization in a disaster.
   (O) Provisions for staff while at off-site location (food, water, telephones, beds, etc.)

   This list of considerations is not all inclusive and must be added to as appropriate.

4. General requirements of contingency plans must include:
   (A) Definitions of conditions under which the Business Recovery Strategy must be implemented.
   (B) Recovery point objective stages.
   (C) Recovery time objective stages.
   (D) Security preservation checklist.
   (E) Task Assignments.
   (F) Post-event Recovery Analysis.
   (G) Required resources, by priority.
   (H) Required recovery time / levels of availability of resources.
   (I) Documentation of normal and response procedures.

5. Refer to the considerations outlined in Appendix D.

8.2 DISASTER RECOVERY PLAN

1. A Disaster Recovery Plan is intended to maintain critical business processes in the event of the loss of any of the following areas for an extended period:
   (A) desktop computers and portable systems,
   (B) servers,
   (C) Web sites,
   (D) local area networks,
   (E) wide area networks,
   (F) distributed systems, and
   (G) mainframe systems.

2. Teams should be formed to address each of the areas indicated consisting of a team lead and designate as well as key knowledge personnel required for that area. All contact information must be available for IT management, team members, all IT personnel and designated business unit management. When available, this information should include:
   (A) work telephone number,
   (B) pager number,
   (C) home telephone number,
   (D) cellular telephone number,
   (E) work email address,
   (F) home email address, and
   (G) home address.

3. Upon receiving the information of a serious incident any member of management can invoke the Plan. Depending on the nature of the incident a command center will be established, and appropriate teams mobilized. Management and the team leads are responsible for contacting all required personnel. Appendix B represents a sample crisis team organization and roles corresponding with potential disaster situations. All roles would have designates in the event one or more individuals are unavailable.

4. Communications to the IT department is the responsibility of Management and the Team Lead. In respect to external communications, it is extremely important

that there is a single point of disclosure to ensure accurate and timely updates. The following roles and individuals must be determined and documented:
(A) Upwards, within the affected agency's organization.
(B) Outwards to affected agencies.
(C) Outwards to the public.

5. Hard copies of the Plan must be:
   (A) stored off site at a secure location,
   (B) stored at the personal residence of the team leads,
   (C) stored at the personal residence of all IT managers and directors, and
   (D) stored on a secure internet site.

6. As soon as an emergency is detected:
   (A) Identify the problem and,
      (i) Notify emergency services in cases of physical threats to personnel or facilities,
      (ii) Notify the IT Director and his alternate.
      (iii) Notify the appropriate team leads. In the event of a mainframe disaster, notify all team leads.
      (iv) Notify vendors and business partners.
   (B) Evacuate the premises if there are concerns of personal safety. All personnel should:
      (i) be aware of evacuation routes and
      (ii) have in possession or be aware of notification numbers.
   (C) Reduce any exposure:
      (i) In the event of air conditioning failure *(this usually involves powering down the systems at a temperature determined by the tolerances set by the manufacturer),*
      (ii) In the event of fire *(this usually involves the automatic releasing of fire retardant, cutting of power, notification to emergency services and evacuation),*
      (iii) In the event of electrical failure *(If a UPS and generator are available, usually the only action is to monitor fuel levels of the generator. If a UPS only is available, shut down procedures should begin and be terminated with at least 20% of rated capacity left),*
      (iv) In the event of flood, water or wind damage *(this usually involves the normal powering down all systems if possible. If not, the immediate cut off of power is required, followed by notification to emergency services and evacuation),*
      (v) In the event of malicious intrusion *(this usually involves the immediate isolation of affected hardware from all networks and*

connectivity. Usually, the extent of exposure and damage is not immediately known so the immediate isolation of all network links is recommended and processing on affected facilities halted pending analysis by crisis teams).

(D) Initiate backup site procedures:
  (i) The Plan Coordinator establishes a command and control center *(usually an onsite and offsite center have been previously identified and the necessary computer and communication links are readily available).*
  (ii) The Plan Coordinator ensures all team leaders are notified *(usually it is the responsibility of the Team Lead to get in touch with all team members).*
  (iii) The Plan Coordinator notifies the off-site storage facility that a contingency event has occurred and to ship the necessary materials as determined in the damage assessment to the alternate site.
  (iv) The Plan Coordinator notifies the alternate site that a contingency event has occurred and to prepare the facility for the organization's arrival.
  (v) Both upward and outward communication on status is the responsibility of the Plan Coordinator *(usually set times are preestablished such as: immediate after 1 hour, after 3 hours, etc. or at major milestones such as problem determination, resolution plan, when planned resumption of services is known and start-up of services is accomplished).*
  (vi) The Plan Coordinator is responsible for managing expectations.

(E) Initiate recovery at the alternate site:
  (i) Contingency plan is followed using documented recovery points and defined priorities.
  (ii) The Plan Coordinator reviews responsibilities with all team members and establishes recovery logs.
  (iii) Recovery goals and procedures are established and prioritized by the Plan Coordinator.

7. The Disaster Plan appendices should include:
  (A) Personnel Contact List
  (B) Vendor Contact List

(C) Equipment and Specifications.
(D) Service Level Agreements.
(E) Related Contracts.
(F) Standard Operating Procedures.

8.3 BUSINESS RECOVERY STRATEGY

1. A Business Recovery Strategy provides the documented organizational plan to restore full business functionality as quickly and as cost-effectively as possible. The Business Recovery Strategy is initiated as soon as the enterprise is deemed able to resume normal operations following a disaster.

2. The Business Recovery Strategy must involve advance planning and preparations to recover from external circumstances. Recovery strategies must be created, implemented, tested and maintained to ensure restoration of organizational services in the event of an interruption.

3. A "worst case scenario" must be the basis for developing the plan, where the worst case scenario is the destruction of the main or primary facility. Because the plan is written based on this premise, less critical situations can be handled by using subsets of the plan, with minor (if any) alterations required. Recovery from, or mitigation of a scenario should not be considered an all-or-nothing proposition. Many stages may be required, each with its own success conditions, before a 'final' state of continuity or recovery is reached.

4. Specific goals of the Business Recovery Strategy must include:
   (A) Complete service functionality recovery objectives, in stages, by delay, duration and degree.
   (B) Details of processes already in place to recover from an incident.
   (C) Details of what degree of business functionality they may be expected to restore.
   (D) In what length of time existing process may be expected to restore service.
   (E) Requirements to bridge from existing processes to sufficient processes.
   (F) Lead time to secure additional resources.

5. The Business Recovery Strategy must include detailed, step-by-step instructions for how to replace / restore the following, in appropriate sequence:
   (A) Applications / Processes
   (B) Functionality / Capacity

(C) Equipment / Infrastructure
(D) Staff /Skills
(E) Execution Duration / Delay
(F) Connectivity / Network
(G) Data Sources
(H) Facilities / Services / Physical Premises
(I) Transportation
(J) Documentation / Reference material

9.0 DATA CENTER MANAGEMENT

1. Related specifically to security of information and data center management, the pace of change, the reality of the World Wide Web and the increasing numbers of internal and external portals demand constant monitoring with both offensive and defensive strategies.

9.1 OPERATING PROCEDURES

1. The operating procedures identified by security procedures should be documented and maintained. Operating procedures should be treated as formal documents and changes authorized by management.

2. The procedures should specify the instructions for the detailed execution of each job including the following:
   (A) processing and handling of information,
   (B) scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times,
   (C) instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities,
   (D) support and owner contacts in the event of unexpected operational or technical difficulties,
   (E) special output handling instructions, such as the use of special stationery or the management of confidential output, including procedures for secure disposal of output from failed jobs, and
   (F) system restart and recovery procedures for use in the event of system failure.

3. Documented procedures should also be prepared for system housekeeping activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, back-up, equipment maintenance, computer room and mail handling management and safety.

9.2 OPERATIONAL CHANGE CONTROL

1. Changes to information processing facilities and systems must be controlled. Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Formal management

responsibilities and procedures should be in place to ensure satisfactory control of all changes to equipment, software or procedures.

2. Operational programs should be subject to strict change control. When programs are changed an audit log containing all relevant information should be retained. Changes to the operational environment can impact applications. Wherever practicable, operational and application change control procedures should be integrated.

3. In particular, the following controls must be implemented:
   (A) identification and recording of significant changes,
   (B) assessment of the potential impact of such changes,
   (C) formal approval procedure for proposed changes,
   (D) communication of change details to all relevant persons, and
   (E) procedures identifying responsibilities for aborting and recovering from unsuccessful changes.

9.3 SEGREGATION OF DUTIES

1. Duties and areas of responsibility must be segregated to reduce opportunities for unauthorized modification or misuse of information or services.

2. Small agencies may find this method of control difficult to achieve, but the principle should be applied as far as is possible and practicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision must be implemented. It is important that security audit remains independent.

3. Care should be taken that no single person can perpetrate fraud in areas of single responsibility without being detected. The initiation of an event should be separated from its authorization.

4. The following controls must be implemented:

(A) It is important to segregate activities which require collusion to defraud, e.g. raising a purchase order and verifying that the goods have been received.
(B) If there is a danger of collusion, then controls need to be devised so that two or more people need to be involved, thereby lowering the possibility of conspiracy.
(C) Separation of duties of both physical and logical access controls must be implemented to separate the access and functions of:
    (i) information systems and infrastructure administration to include configuration.
    (ii) security, audit, and accountability functions.
    (iii) privileged users and power user functions;
    (iv) data analysis and report generation functions.
    (v) general user functionality and associated access must be segregation between user and administrative functions and access must be maintained.

9.4 SEPARATION OF DEVELOPMENT AND OPERATIONAL FACILITIES

1. Development and testing facilities must be separated from operational facilities. Rules for the transfer of software from development to operational status should be defined and documented.

2. Development and test activities can cause serious problems, e.g. unwanted modification of files or system environment or of system failure. The level of separation that is necessary, between operational, test and development environments, to prevent operational problems should be considered. A similar separation should also be implemented between development and test functions. In this case, there is a need to maintain a known and stable environment in which to perform meaningful testing and to prevent inappropriate developer access.

3. Where development and test staff have access to the operational system and its information, they may be able to introduce unauthorized and untested code or alter operational information. On some systems this capability could be misused to commit fraud or introduce untested or malicious code. Untested or malicious code can cause serious operational problems.

4. Developers and testers also pose a threat to the confidentiality of operational information. Development and testing activities may cause unintended changes to software and information if they share the same computing environment. Separating development, test and operational facilities is therefore desirable to reduce the risk of accidental change or unauthorized access to operational software and business information.

5. The following controls should be considered:
   (A) Development and operational software should, where possible, run on different computer processors, or in different domains or directories.
   (B) Development and testing activities should be separated the best way possible.
   (C) Compilers, editors and other system utilities should not be accessible from operational systems.
   (D) Different log-on procedures should be used for operational and test systems, to reduce the risk of error. Users should be encouraged to use different passwords for these systems and menus should display appropriate identification messages.
   (E) Development staff should only have access to operational passwords where controls are in place for issuing passwords for the support of operational systems. Controls should ensure that such passwords are changed after use.

9.5 SYSTEMS PLANNING AND ACCEPTANCE

1. To minimize the risk of systems failure:
   (A) Planning and preparation are required to ensure the availability of adequate capacity and resources.
   (B) Projections of future capacity requirements should be made, to reduce the risk of system overload.
   (C) The operational requirements of new systems should be established, documented and tested prior to their acceptance and use.

9.6 CAPACITY PLANNING

1. Capacity demands must be monitored, and projections of future capacity requirements made to ensure that adequate processing power and storage are available. These projections should take account of new business and system requirements and current and projected trends in the organization's information processing.

2. Mainframe computers require particular attention, because of the much greater cost and lead time for procurement of new capacity. Operations managers of mainframe services should monitor the utilization of key system resources, including processors, main storage, file storage, printers and other output devices and communications systems. They should identify trends in usage, particularly in relation to business applications or management information system tools.

3. These managers should use this information to identify and avoid potential bottlenecks that might present a threat to system security or user services and plan appropriate remedial action.

9.7 SYESTEMS ACCEPTANCE

1. Acceptance criteria for new information systems, upgrades and new versions must be established and suitable tests of the system carried out prior to acceptance. Operations managers should ensure that the requirements and criteria for acceptance of new systems are clearly defined, agreed, documented and tested.

2. The following controls should be considered:
   (A) performance and computer capacity requirements,
   (B) error recovery and restart procedures and contingency plans,
   (C) preparation and testing of routine operating procedures to defined standards,
   (D) agreed set of security controls in place,
   (E) effective manual procedures,
   (F) business continuity arrangements as required,
   (G) evidence that installation of the new system will not adversely affect existing systems, particularly at peak processing times, such as month end,
   (H) evidence that consideration has been given to the effect the new system has on the overall security of the organization, and
   (I) training in the operation or use of new systems.

3. For major new developments, the operations function and users should be consulted at all stages in the development process to ensure the operational efficiency of the proposed system design. Appropriate tests should be carried out to confirm that all acceptance criteria are fully satisfied.

9.8 OPERATIONS AND FAULT LOGGING

1. Operational staff must maintain a log of their activities. Logs should include as appropriate:
   (A) system starting and finishing times,
   (B) system errors and corrective action taken,
   (C) confirmation of the correct handling of data files and computer output, and
   (D) the name of the person making the log entry.

2. Faults must be reported, and corrective action taken. Faults reported by users regarding problems with information processing or communications systems should be logged. There should be clear rules for handling reported faults including:
   (A) review of fault logs to ensure that faults have been satisfactorily resolved, and
   (B) review of corrective measures to ensure that controls have not been compromised and that the action taken is fully authorized.

9.9 MANAGEMENT OF REMOVABLE COMPUTER MEDIA

1. Appropriate operating procedures must be established to protect documents, computer media (tapes, disks, cassettes, etc.), input/output data, and system documentation from damage, theft and unauthorized access. The following procedures should be followed:
   (A) If no longer required, the previous contents of any re-usable media that are to be removed from the organization should be erased.
   (B) Authorization should be required for all media removed from the organization and a record of all such removals maintained.

(C) All media should be stored in a safe, secure environment, in accordance with manufacturers' specifications.
(D) All procedures and authorization levels should be clearly documented.

9.10 DISPOSAL OF MEDIA

1. Formal procedures for the secure disposal of media should be established to minimize this risk. The following controls should be considered:
   (A) Media containing sensitive information should be stored and disposed of securely and safely, e.g. by incineration or shredding or emptied of information for use by another application within the organization.
   (B) The following list identifies items that might require secure disposal:
      (i) paper documents,
      (ii) voice or other recordings,
      (iii) output reports,
      (iv) one-time-use printer ribbons,
      (v) magnetic tapes,
      (vi) removable disks or cassettes,
      (vii) optical storage media (all forms and including all manufacturer software distribution media),
      (viii) program listings,
      (ix) test information, and
      (x) system documentation.

   (C) It may be easier to arrange for all media items to be collected and disposed of securely, rather than attempting to separate out the sensitive items.
   (D) Disposal of sensitive items should be logged where possible to maintain an audit trail.
   (E) Disposal of certain hardware must conform to the current EPA requirements or other relevant legislation in effect.

9.11 EXCHANGES OF INFORMATION AND SOFTWARE

1. Exchanges of information and software between organizations should be controlled and should be compliant with any relevant legislation.

2. Exchanges should be carried out based on agreements. Procedures and standards to protect information and media in transit must be established. The

business and security implications associated with electronic data interchange, electronic commerce and electronic mail and the requirements for controls should be considered.

3. Agreements, some of which must be formal, must be established for the electronic or manual exchange of information and software between organizations. The security content of such an agreement should reflect the sensitivity of the business information involved. Agreements on security conditions should include:
   (A) responsibilities for controlling and notifying transmission, dispatch and receipt,
   (B) procedures for notifying sender, transmission, dispatch and receipt,
   (C) minimum technical standards for packaging and transmission,
   (D) courier identification standards,
   (E) responsibilities and liabilities in the event of loss of information,
   (F) information and software ownership and responsibilities for information protection, software copyright compliance and similar considerations,
   (G) technical standards for recording and reading information and software, and
   (H) any special controls that may be required to protect sensitive items, such as cryptographic.

4. Information can be vulnerable to unauthorized access, misuse or corruption during physical transport, for instance when sending media via the postal service or via courier. As such, media being transported must be protected from unauthorized access, misuse or corruption.

9.12 PUBLICLY AVAILABLE SYSTEMS

1. Information on a publicly available system, e.g. information on a Web server accessible via the Internet, may need to comply with laws, rules and regulations in the jurisdiction in which the system is located or where trade is taking place. There must be a formal authorization process before information is made publicly available and the integrity of such information must be protected to prevent unauthorized modification.

2. Software, data and other information requiring a high level of integrity, made available on a publicly available system, should be protected by appropriate mechanisms, e.g. digital signatures. Electronic publishing systems, especially those that permit feedback and direct entering of information, should be carefully controlled so that:
   (A) information is obtained in compliance with any information protection legislation,
   (B) information input to and processed by the publishing system will be processed completely and accurately in a timely manner,
   (C) sensitive information will be protected during the collection process and when stored, and
   (D) access to the publishing system does not allow unintended access to networks to which it is connected.

9.13 USE OF SYSTEM UTILITIES

1. Most computer installations have one or more system utility programs that might be capable of overriding system and application controls. Use of these system utility programs must be restricted and tightly controlled. The following controls should be considered:
   (A) use of authentication procedures for system utilities,
   (B) segregation of system utilities from applications software,
   (C) limitation of the use of system utilities to the minimum practical number of trusted authorized users,
   (D) authorization for ad hoc use of systems utilities,
   (E) limitation of the availability of system utilities, e.g. for the duration of an authorized change,
   (F) logging of all use of system utilities,
   (G) defining and documenting of authorization levels for system utilities, and
2. removal of all unnecessary software-based utilities and system software.

9.14 MONITORING SYSTEMS ACCESS AND USE

1. Systems should be monitored to detect deviation from access control procedures and record system events to provide evidence in case of security incidents. System monitoring allows the effectiveness of controls adopted to be checked.

2. Audit logs recording exceptions and other security-relevant events must be produced and kept for a period defined by the hosting Office or Department and within the mandate of both federal and State legislation to assist in future investigations and access control monitoring. Audit logs should also include:
   (A) user IDs,
   (B) dates and times for log-on and log-off,
   (C) terminal identity or location if possible,
   (D) records of successful and rejected system access attempts, and
   (E) records of successful and rejected data and other resource access attempts.

3. Certain audit logs may be required to be archived as part of the record retention procedures or because of requirements to collect evidence.

4. Procedures for monitoring use of information processing facilities must be established and the result of the monitoring activities reviewed regularly. Such procedures are necessary to ensure that users are only performing activities that have been explicitly authorized. The level of monitoring required for individual facilities should be determined by a risk assessment. Areas that should be included are:
   (A) authorized access, including detail such as:
      (i) the user ID,
      (ii) the date and time of key events,
      (iii) the types of events,
      (iv) the files accessed, and
      (v) the program/utilities used.
   (B) all privileged operations, such as:
      (i) use of supervisor account,
      (ii) system start-up and stop, and
      (iii) I/O device attachment/detachment.
   (C) unauthorized access attempts, such as:
      (i) failed attempts,
      (ii) access procedure violations and notifications for network gateways and firewalls, and
      (iii) alerts from proprietary intrusion detection systems.

(iv)
(D) system alerts or failures such as:
(i) console alerts or messages,
(ii) system log exceptions, and
(iii) network management alarms.

5. The result of the monitoring activities should be reviewed regularly. The frequency of the review should depend on the risks involved. Risk factors that should be considered include:
   (A) the criticality of the application processes,
   (B) the value, sensitivity or criticality of the information involved,
   (C) the past experience of system infiltration and misuse and
   (D) the extent of system interconnection (particularly public networks).

6. A log review involves understanding the threats faced by the system and the way these may arise. System logs often contain a large volume of information, much of which is extraneous to security monitoring. To help identify significant events for security monitoring purposes, the copying of appropriate message types automatically to a second log and/or the use of suitable system utilities or audit tools to perform file interrogation should be considered. When allocating the responsibility for log review a separation of roles should be considered between the person(s) undertaking the review and those whose activities are being monitored.

7. Particular attention should be given to the security of the logging facility because if tampered with it can provide a false sense of security. Controls should aim to protect against unauthorized changes and operational problems including:
   (A) the logging facility being de-activated,
   (B) alterations to the message types that are recorded,
   (C) log files being edited or deleted, and
   (D) log file media becoming exhausted and either failing to record events or overwriting itself.

9.15 CONTROL OF OPERATIONAL SOFTWARE

1. Control must be applied to the implementation of software on operational systems. To minimize the risk of corruption of operational systems, the following controls should be considered:

(A) The updating of the operational program libraries should only be performed by the nominated librarian upon appropriate management authorization.
(B) Operational systems should only hold executable code.
(C) Executable code should not be implemented on an operational system until evidence of successful testing and user acceptance is obtained and the corresponding program source libraries have been updated.
(D) An audit log should be maintained of all updates to operational program libraries.
(E) Previous versions of software should be retained as a contingency measure.

2. Vendor supplied software used in operational systems should be maintained at a level supported by the supplier. Any decision to upgrade to a new release should consider the security of the release, i.e. the introduction of new security functionality or the number and severity of security problems affecting this version. Software patches should be applied when they can help to remove or reduce security weaknesses.

9.16 ACCESS CONTROL TO SOURCE LIBRARY

1. To reduce the potential for corruption of computer programs, strict control must be maintained over access to program source libraries.
   (A) Program source libraries should not be held in operational systems.
   (B) A program librarian should be nominated for each application.
   (C) IT support staff should not have unrestricted access to program source libraries.
   (D) Programs under development or maintenance should not be held in operational program source libraries.
   (E) The updating of program source libraries and the issuing of program sources to programmers should only be performed by the nominated librarian upon authorization from the IT support manager for the application.
   (F) Program listings should be held in a secure environment.

(G) An audit log should be maintained of all accesses to program source libraries.
(H) Old versions of source programs should be archived, with a clear indication of the precise dates and times when they were operational, together with all supporting software, job control, data definitions and procedures.
(I) Maintenance and copying of program source libraries should be subject to strict change control procedures.

9.17 CHANGE CONTROL PROCEDURES

1. The implementation of changes must be strictly controlled using formal change control procedures to minimize the risk of system corruption. These formalized change controls must be enforced. They should ensure that security and control procedures are not compromised, that programmers are given access to only those units required for their work and that formal approvals are obtained. Changing application software can impact the operational environment. Whenever practical, application and operational change procedures should be integrated.
   These processes should include:
   (A) maintaining a record of agreed authorization levels,
   (B) ensuring changes are submitted by authorized personnel,
   (C) reviewing controls and procedures to ensure they will not be compromised by the changes submitted,
   (D) identifying all the software, databases and hardware that require change,
   (E) obtaining formal approval before work commences,
   (F) ensuring the changes are carried out to minimize any possible disruptions,
   (G) ensuring the system documentation is current,
   (H) maintaining version control on all updates,
   (I) maintaining an audit trail of all change requests,
   (J) ensuring that operational documentation and user procedures reflect the new environment, and
   (K) ensuring that the changes are implemented without business disruption.

2. Test environments should be separated from development and production environments.

9.18 RESTRICTIONS ON CHANGES TO SOFTWARE

1. Modification to software packages must be discouraged and essential changes controlled. Only when deemed essential, should the packages be modified. The following points should be considered:
   (A) the possibility of controls and processes included in the base software being compromised,
   (B) the necessity of obtaining the vendor's consent,
   (C) the possibility of the vendor including the changes into the base offering, and
   (D) the impact of incorporating these changes in future releases of the base software.

9.19 INTRUSION DETECTION SYSTEMS (IDS)

1. Network IDS utilize traffic analysis to compare session data against a known database of popular application attack signatures. On detection, the network IDS can react by logging the session alerting the administrator, terminating the session and even reconfiguring the firewall or router to block selected traffic.

2. Host IDS compare application / internal service log events against a known database of security violations and custom policies. If a breach of policy occurs, the host IDS can react by logging the action alerting the administrator and, in some cases, stopping the action prior to execution.

3. Application-Level IDS rely upon custom applications to log unauthorized or suspect activity and / or produce an alert. An example of an Application-Level IDS would be a Web application which maintains its own internal user / password system. Attempts to circumvent this system would not be noticed by a Network IDS or recorded by a Host IDS.

9.20 CONTROLS ON MALICIOUS SOFTWARE

1. Detection and prevention controls to protect against malicious software and appropriate user awareness procedures must be implemented. Protection against malicious software should be based on security awareness

appropriate system access and change management controls. The following procedures should be implemented:

(A) compliance with software licenses and prohibiting the use of unauthorized software,

(B) protection against risks associated with obtaining files and software either from or via external networks or on any other medium, indicating what protective measures should be taken,

(C) installation and regular update of anti-virus detection and repair software to scan computers and media either as a precautionary control or on a routine basis,

(D) regular reviews of the software and information content of systems supporting critical business processes—the presence of any unapproved files or unauthorized amendments should be formally investigated,

(E) verification of files on electronic media of uncertain or unauthorized origin, or files received over un-trusted networks, for viruses before use,

(F) verification of any electronic mail attachments and downloads for malicious software before use—this check may be carried out at different places, e.g. at electronic mail servers, desk top computers or when entering the network of the organization,

(G) assignment of responsibilities to deal with the virus protection on systems, training in their use, reporting and recovering from virus attacks,

(H) appropriate business continuity plans for recovering from virus attacks, including all necessary data and software back-up and recovery arrangements,

(I) verification of all information relating to malicious software and ensure that warning bulletins are accurate and informative, and

(J) verification that qualified sources, e.g. reputable journals, reliable Internet sites or anti-virus software suppliers are used to differentiate between hoaxes and real viruses.

2. Staff should be made aware of the problem of hoaxes and what to do on receipt of them. These controls are especially important for network file servers supporting large numbers of workstations.

9.21 FIREWALLS

1. Firewalls' functionality must be documented and detail how they manage security policy as applied to network traffic and how they maintain internal security.

2. System documentation must detail the following:
   (A) Purpose / Business rationale for the system
   (B) Services offered, including business rationale.
   (C) Rationale for the choice of platform, operating system, components and configuration.
   (D) Adjacent or integrated systems.
   (E) Modifications to the default system software configuration
   (F) Installed software.
   (G) Installed software configuration.
   (H) Installed hardware.
   (I) Installed hardware configuration.
   (J) Support contracts.
   (K) Software licenses
   (L) Hardware lease details
   (M) Procedures for shutdown, restart and recovery
   (N) System maintenance schedule

9.22 EXTERNAL FACILITIES MANAGEMENT

1. The use of an external contractor to manage information processing facilities may introduce potential security exposures, such as the possibility of compromise, damage, or loss of data at the contractor's site. Prior to using external facilities management services, the risks must be identified, and appropriate controls agreed with the contractor, and incorporated into the contract.

2. Issues that should be addressed include:
   (A) identifying sensitive or critical applications better retained in-house,
   (B) obtaining the approval of business application owners,
   (C) implications for business continuity plans,
   (D) security standards to be specified, and the process for measuring compliance,
   (E) allocation of specific responsibilities and procedures to effectively monitor all relevant security activities, and
   (F) responsibilities and procedures for reporting and handling security incidents.

10.0 LEGAL REQUIREMENTS

1. All security related aspects of information processing may be subject to statutory or contractual security requirements. Each Office or Department must be aware of their responsibilities as dictated by legislation and other legal commitments particularly as they apply to the information systems and practices required by the federal and state governments. All Offices and Departments should put in place the appropriate procedures to ensure compliance with legal considerations.

10.1 SOFTWARE COPYRIGHT

1. Proprietary software products are usually supplied under a license agreement that limits the use of the products to specified machines and may limit copying to the creation of back-up copies only. The following controls should be implemented:
   (A) publishing software copyright compliance procedures which define the legal use of software and information products,
   (B) maintaining awareness of the software copyright and acquisition procedures and giving notice of the intent to take disciplinary action against staff who breach them,
   (C) maintaining appropriate asset registers,
   (D) maintaining proof and evidence of ownership of licenses, master disks, manuals, etc.,
   (E) implementing controls to ensure that any maximum number of users permitted is not exceeded,
   (F) carrying out checks that only authorized software and licensed products are installed,
   (G) providing procedures for maintaining appropriate license conditions, and
   (H) providing procedures for disposing or transferring software to others.

10.2 PROTECTION OF INFORMATION

1. Important records of an organization must be protected from loss, destruction and falsification. Some records may need to be securely retained to meet statutory or regulatory requirements as well as to support essential business activities. The time period and information content for retention may be set by federal and state laws or regulations. The Owning Office or Department is responsible for notifying the Hosting Office or Department of any requirements to be met.

2. Records should be categorized into record types, such as accounting records, database records, transaction logs audit logs and operational procedures, each

with details of retention periods and type of storage media, e.g. paper, microfiche, magnetic, optical. Any related cryptographic keys associated with encrypted archives or digital signatures, should be kept securely and made available to authorized persons when needed.

3. Consideration should be given to the possibility of degradation of media used for storage of records. Storage and handling procedures should be implemented in accordance with Manufacturer's recommendations.

4. Wherever electronic storage media are chosen, procedures to ensure the ability to access information (both media and format readability) throughout the retention period should be included, to safeguard against loss due to future technology change.

5. The system of storage and handling should ensure clear identification of records and of their statutory or regulatory retention period. It should permit appropriate destruction of records after that period if they are not needed by the organization.

6. To meet these obligations, the following steps should be taken within an organization:
   (A) Guidelines should be issued on the retention, storage, handling and disposal of records and information.
   (B) A retention schedule should be drawn up identifying essential record types and the period of time for which they should be retained.
   (C) An inventory of sources of key information should be maintained.
   (D) Appropriate controls should be implemented to protect essential records and information from loss, destruction and falsification.

10.3 PRIVACY OF PERSONAL INFORMATION

1. In many cases, legislation controls the processing and transmission of personal information (generally information on living individuals who can be identified from that information). Such controls impose responsibilities on those collecting, processing and disseminating personal information.

2. Controls must be applied to protect personal information in accordance with relevant legislation. Compliance with information protection legislation requires appropriate management structure and control. It is the responsibility of the owner of the

information to ensure the information is protected and that there is awareness by all users of the information protection principles defined in the relevant legislation.

11.0 COMPLIANCE WITH SECURITY POLICY

1. Offices and Departments must ensure that all security procedures within their area of responsibility are documented and carried out correctly. All areas within the organization may be subject to regular review to ensure compliance with security procedures and standards. These should include the following:
   (A) information systems,
   (B) systems providers,
   (C) owners of information and information assets,
   (D) hosting agencies of information and information assets, and
   (E) users.

2. Both the owning and hosting agencies should support regular reviews of the compliance of their systems with the appropriate security procedures, standards and any other security requirements. All variances must be documented.

APPENDIX A: GLOSSARY

Backup: A copy of files and programs made to facilitate recovery if necessary.

Business Continuity: The predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption of the normal business environment.

Business Recovery Strategy: The documentation of a predetermined set of instructions or procedures that describe how business processes will be restored after a significant disruption to the normal business environment has occurred.

Cold Site: A backup facility that has the necessary electrical and physical components of a computer facility but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment if the user has to move from their main computing location to an alternate site.

Contingency Plan: Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures or disaster.

Critical Application: An application that requires special attention to security because of the risk and magnitude of the harm resulting from the loss, misuse or unauthorized access to, or modification of, the information in the application. A breach in a critical application might comprise many individual application programs and hardware, software and telecommunications components. Critical applications can be either a major software application or a combination of hardware and software in which the only purpose of the system is to support a specific mission-related function.

Disaster Recovery Plan: An information technology plan designed to restore operability of the target system, application, telecommunication, or computer facility after a major hardware or software failure or destruction of facilities.

Disruption: An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage,

extended unavailable network, equipment or facility damage or destruction, or corruption of files by accidental or malicious intent).

Distributed System: A distributed system is an interconnected set of multiple autonomous processing units, configured to exchange and process information to complete a single business function. To the user a distributed system appears to be a single source. Distributed systems use the client-server relationship model to make the application more accessible to users in different locations.

Environmental Considerations: Those physical or tangible factors that affect the performance of, or compliance with, a given procedure or process.

Facilities: Interconnected information resources that share common functionality. They include hardware, software, information, information applications and communications.

Functional Considerations: Those process or procedure factors that affect the performance of, or compliance with, a given function.

Hosting Office or Department: The Hosting Office or Department has physical and operational control of the hardware, software, communications and databases (files) of the owning Office or Department. The Hosting Office or Department can also be an Owner.

Hot Site: A fully operational off-site information processing facility equipped with hardware and system software to be used in the event of a disaster.

Incident: A malicious attack against an organization's IT systems. It is normally associated with cyber attacks but includes any unauthorized violation of policies and procedures.

Information: Any data or knowledge collected, processed, stored, managed, transferred or disseminated by any method.

Intrusion Detection System: The function of an Intrusion Detection System (IDS) is to monitor and analyze captured activity data and issue alerts when unauthorized activity is detected. The functionality of the IDS must be documented as well as details on how the IDS discovers, filters and reports events based on guidelines set by security policy.

Local Area Network (LAN): A local area network (LAN) is a data communications network owned by a single organization. It can be as small as two PCs attached or can include hundreds of users and multiple servers.

Mainframe: A mainframe is a multi-user computer designed to meet the computing needs of a large organization. The term was created to describe the large central computers developed in the late 1950s and 1960s to process bulk accounting and information management functions. Mainframe systems store most, if not all data in a central location rather than dispersing data among multiple machines as with distributed systems.

Owner: The Owner of the information is the County Office or Department responsible for producing, collecting and maintaining the authenticity, integrity and accuracy of information.

Risk Management: Risk management is the ongoing process of assessing, controlling and mitigating the risks to information systems and technologies. Risk management should prevent or reduce the likelihood of damage to its information resources through implementation of security controls to protect a system or technologies against natural, human and environmental threats. Risk management should encompass actions to reduce or limit the consequences of risks in the event they disrupt a system or technological component.

Security Representative: An individual designated by a County Office or Department to approve user access, communicate security policies, procedures, guidelines and best practices to personnel, and report on all deviations to security policies, procedures, guidelines and best practices.

Server: A server is a computer that runs software to provide access to a resource or part of the network and network resources, such as disk storage, printers and network applications. A server can be any type of computer running a network operating system. A server may be a standard PC or it can be a large computer containing multiple disk drives and a vast amount of memory that will allow the computer to process multiple, concurrent requests.

Service Level Agreement: A documented commitment on products, services or service levels to be provided. This must be agreed upon by the provider as well as the recipient and serves to manage expectations and monitor performance.

Shared Network: A network shared with third party or non-organizational users.

System: A generic term used for briefness to mean either a major application or a general support system.

Systems Access Authorization Request: Documented authorization for an individual's system access signed and approved by the requesting manager, the designated Security Representative and the Owner.

System Development Life Cycle: The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance and ultimately its disposal that instigates another system initiation.

Vetting: Verification of information or individuals associated with the process or task assigned.

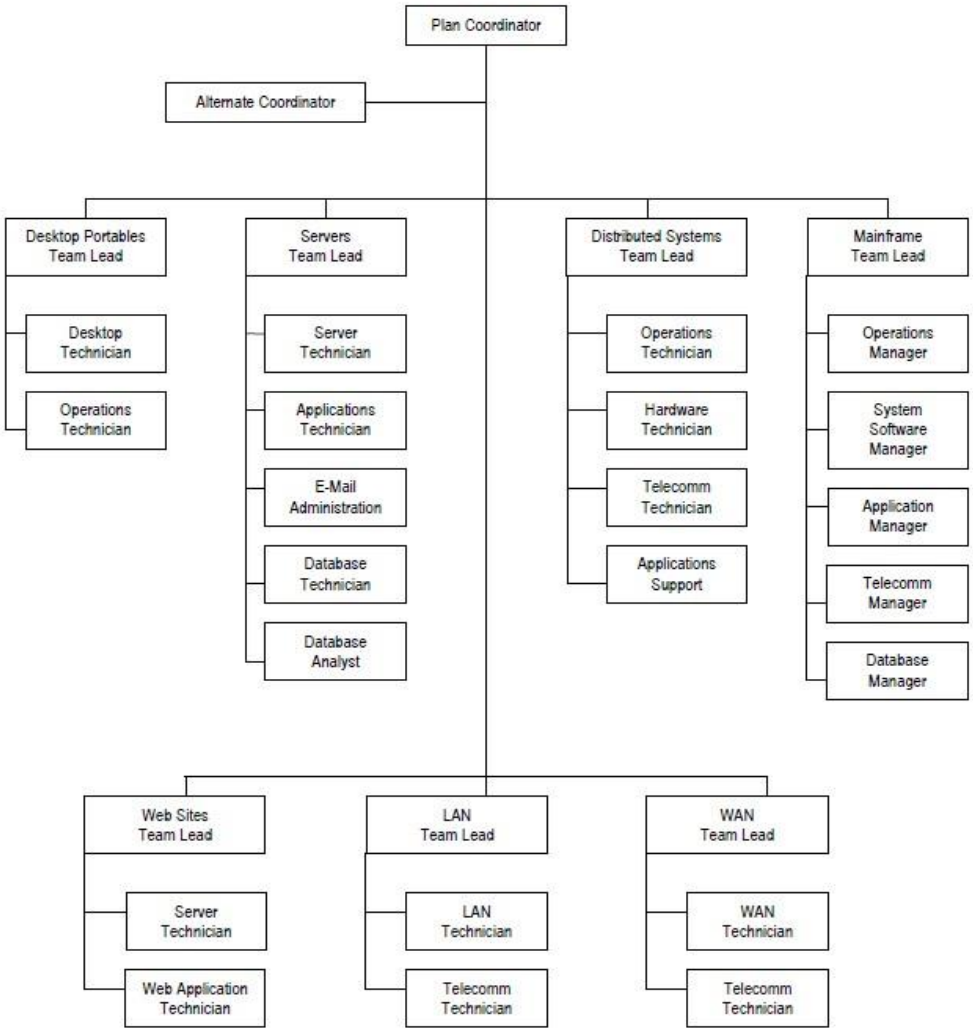
Warm Site: An environmentally conditioned workspace that is partially equipped with IT and telecommunications equipment to support relocated IT operations in the event of a significant disruption.

Web Site: A Web site is used for information dissemination on the Internet or an intranet. The Web site is created in Hypertext Markup Language (HTML) code that may be read by a Web browser on a client machine. A Web site is hosted on a computer (Web server) that serves Web pages to the requesting client browser. The Web server hosts the components of a Web site (e.g., pages, scripts, programs and multimedia files) and serves them using the Hypertext Transfer Protocol (HTTP). Web sites can present static or dynamic content. A Web site can be either internal to an organization (an intranet) or published to the public over the Internet.

Wide Area Network (WAN): A wide area network (WAN) is a data communications network that consists of two or more LANs that are dispersed over a wide geographical area. Communications links, usually provided by a public carrier, enable one LAN to interact with other LANs.

APPENDIX B: SAMPLE CRISIS TEAM ORGANIZATION

The following sample illustrates crisis team compositions insofar as skills mix required for the disaster recovery components. Alternates should be assigned for all critical skills.



APPENDIX C: RESPONSIBILITY GRID

The following grid outlines the primary responsibilities **(in bold)** for all the security considerations listed in the Policy, Procedures, and Guidelines document. In addition, the considerations are applied to the major components listed under disaster recovery. This does not preclude the fact that all State employees and agencies share in all responsibilities pertaining to information security.

Security Considerations	**Users**	**Owner**	**Host**	Desktops	Servers	Web Sites	LAN	WAN	Dist. Sys.	Mainframe
Information Confidentiality	**x**	**x**	**x**	x	x	x	x	x	x	x
Information Content		**x**		x	x	x			x	x
Information Access		**x**	**x**	x	x	x				x
Information Security		**x**		x	x	x			x	x
Information Availability			**x**	x	x	x	x	x	x	x
Hosting Office/Department Security			**x**	x	x	x	x	x	x	x
Owning Office/Department Security	**x**	**x**	**x**	x	x	x	x	x	x	x
Incident Management		**x**	**x**	x	x	x	x	x	x	x
Event Logging and Monitoring			**x**		x	x	x	x	x	x
Risk Assessment			**x**	x	x	x	x	x	x	x
Risk Mitigation			**x**	x	x	x	x	x	x	x
Staffing			**x**		x	x	x	x	x	x
Awareness/Training		**x**	**x**	x	x	x	x	x	x	x
Personal Computer Usage	**x**	**x**		x						
Email Usage	**x**	**x**	**x**	x			x	x		
Internet/Intranet Security			**x**		x	x				
Support Calls			**x**		x	x	x	x	x	x
Password Resets		**x**	**x**		x				x	x
Voice Mail Security		**x**	**x**					x		
Operations Center			**x**	x	x	x	x	x		x
Operations Monitoring			**x**		x	x	x	x	x	x
Back Up of Information	**x**		**x**	x	x				x	x

Access Control			**x**	x	x	x	x	x	x	x
Network			**x**				x	x	x	
Electronic Commerce Security			**x**		x		x	x	x	x
Mobile Computing	**x**		**x**	x					x	
Remote Computing			**x**	x	x	x		x	x	
External Facilities			**x**	x	x	x	x	x	x	x
Encryption		**x**	**x**	x	x		x	x	x	x
Contingency Plan		**x**	**x**		x	x	x	x	x	x
Disaster Recovery Plan		**x**	**x**		x	x	x	x	x	x
Business Recovery Strategy		**x**	**x**		x	x	x	x	x	x

Security Considerations	**Users**	**Owner**	**Host**	Desktops	Servers	Web Sites	LAN	WAN	Dist. Sys.	Mainframe
Operating Procedures			**x**		x	x	x	x	x	x
Operational Change Control			**x**		x	x	x	x	x	x
Segregation of Duties			**x**		x				x	x
Separation of Development & Operational Facilities			**x**		x				x	x
Systems Planning & Acceptance			**x**		x				x	x
Capacity Planning			**x**	x	x		x	x	x	x
Systems Acceptance			**x**		x	x	x	x	x	x
Fault Logging			**x**		x				x	x
Management of Removable Computer Media		**x**	**x**		x				x	x
Disposal of Media	**x**	**x**	**x**	x	x				x	x
Exchanges of Information & Software		**x**	**x**		x		x	x	x	x

Publicly Available Systems		**x**			x	x				x
Use of System Utilities			**x**		x				x	x
Monitoring Systems Access & Use		**x**	**x**	x	x	x	x	x	x	x
Control of Operational Software			**x**		x				x	x
Access Control to Source Library			**x**		x					x
Change Control Procedures			**x**		x				x	x
Restrictions on Changes to Software			**x**		x				x	x
Intrusion Detection Systems (IDS)			**x**		x				x	x
Controls on Malicious Software			**x**		x				x	x
Firewalls		**x**	**x**	x	x				x	x
External Facilities Management			**x**	x	x	x	x	x	x	x
Software Copyright	**x**	**x**	**x**	x	x				x	x
Protection of Information	**x**	**x**	**x**	x	x	x	x	x	x	x
Privacy of Personal Information	**x**	**x**	**x**	x	x				x	x
Compliance with Security Policy	**x**	**x**	**x**	x	x	x	x	x	x	x

APPENDIX D: CONTINGENCY PLAN CONSIDERATIONS

Maintain an up to date inventory of hardware and software.
Standardize hardware, software, and peripherals.
Coordinate with security policies and procedures.
Backup and storage of critical information offsite.
Ensure interoperability among system components.
Implement redundancy in critical system components.
Use uninterruptible power supplies.
Document system and application configurations
Document environmental requirements.
Backup and storage of information and applications offsite.

Implement fault tolerance in critical system components.
Replicate information.
Document Web site.
Code and program the Web site uniformly.
Consider contingencies of supporting infrastructure.
Implement load balancing
Coordinate with incident response procedures.
Document the network
Coordinate with vendors.
Identify single points of failure.
Monitor the network
Institute service level agreements
Consider a hot site or reciprocal agreement.

APPENDIX E: REVISIONS

County Request No. 262

REQUEST FOR LEGAL SERVICES

This form is used to provide legal opinions and contract approval by the District Attorney's Office. Only that advice that is related to a pending or potential claim against the County or its officers and employees is protected by the attorney-client priviledge. Opinions that are privileged should not be disclosed to anyone or the priviledge may be waived.

All legal opinions and approvals rendered are based only on the documentation and information stated below or attached to this form and, thus, it is important that all relevant facts and information be provided at the time of review. Please advise the District Attorney's Office of new or additional information, as it may cause the opinion to change. In all cases, the opinions of the District Attorney's Office are not binding on the County, its officers or employees and may be followed or disregarded in the discretion of the elected official.

Date of Request: 05/08/2024 Department: D3

State the nature of the legal request:

Does the OK County InfoSec Policy violate any federal or Oklahoma law

RECEIVED

MAY 08 2024

CIVIL DIVISION
DISTRICT ATTORNEY

Colton Murphy

County Officer or Department Director

Reply of District Attorney's Office:

Reviewed - DK

Date of Reply: 5/8/24

Assistant District Attorney