CONTRA COSTA COUNTY
Office of the County Administrator
ADMINISTRATIVE BULLETIN

Number: 140
Date: March 17th, 2008
Section: Information Security Technology Policy

SUBJECT: INFORMATION SECURITY – INFORMATION TECHNOLOGY POLICY

The purpose of this policy is to outline the use and need for protection of information maintained in the County. These guiding principles are in place to mutually protect the employees and the County as a whole. Inappropriate use exposes the County to risks including malicious attacks, compromise of network systems and services, and legal issues**.**

I. APPLICABILITY

This policy applies to employees, contractors, consultants, temporaries, and other workers at the County, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the County, or connects to the County network.

Effective security is a team effort involving the participation and support of every County employee and affiliate who deals with information and/or information systems. Every computer user must know this policy and conduct their activities in compliance with it.

II. AUTHORITY

Formally adopted by the Board of Supervisors on March 23rd, 2004, the Countywide Information Security Program has been operating on an administrative level since 1997. The Information Security Program was compiled using information from the International Organization for Standardization's (ISO) Code of Practice for Information Security Management (ISO17799), State and Federal Statutes, the California Counties Information Services Directors Association Information Security Forum's members' expertise and experience, the National Security Agency (NSA), the National Institute of Standards and Technology (NIST), and the Generally Accepted Systems Security Principles (GASSP). It outlines industry-proven components that constitute a comprehensive program.

Delegation of Authority to the Chief Information Security Officer is the key to the development and enforcement of the County's comprehensive Information Security Program (ISP). This position will ensure the continuous development

and review of County-wide policies and assist departments in the development of procedures for adherence to the ISP.

III. DESCRIPTION OF POLICY

A. RESOURCE AUDIT

The purpose of this guideline is to provide the authority for staff representing the County Information Technology (I.T.) organizations to conduct a security audit on any computing resource of the County.

1. Audit Purpose
   a. Ensure integrity, confidentiality, and availability of information and resources.
   b. Investigate possible security incidents to ensure conformance to County IT and security policies.
   c. Monitor user or system activity where appropriate.
   d. Verify that software patching is being maintained at the appropriate security level.
   e. Verify virus protection is being maintained at current levels.
   f. Validate compliance with stated security policies.

2. System Access
   a. When requested, and for the purpose of performing an audit, any access needed will be provided to staff representing the internal auditor or as directed by the department head e.g., user level and/or system level access to any computing or communications device.
   b. Access to information (electronic, hardcopy, etc.) that may be produced, transmitted, or stored on County IT equipment or premises.
   c. Access to work areas e.g., labs, offices, cubicles, storage areas, etc.
   d. Access in order to interactively monitor and log traffic on any County network.

B. BACKUP and RECOVERY

The purpose of this guideline is to ensure the safety and recoverability of County information assets by outlining best practices and recommendations for backup and storage of these assets.

1. System Backup
   a. Backup procedures are decided on a departmental basis according to the levels of criticality and changeability of the subject data. The schedule of data backup should be determined by the Departmental Information Security Representative (DISR) and carried out by the department's IT staff or vendor, or other personnel designated and trained to perform backup and recovery. Once a backup schedule is

set, test the backup process from start to finish, determining whether data and its prerequisite application(s) and operating system(s) can be recovered.

b. Backups are written to various forms of media. Regardless of form used, the media must be replaced at intervals sufficient to guarantee its integrity. Backup operators should be aware of whether the media in use is compatible with the alternate computer system to be used following a disaster, considering storage density, media type, and type of tape or disk drive.

c. It is imperative that offsite storage be arranged to house at least one current copy of all critical data, along with documentation outlining the complete restoration of the data and its supporting application(s) and operating system(s). Multiple copies of the data are encouraged to ensure recoverability. Consideration should be made when selecting an offsite storage location for the sufficiency of geographical distance from the original site, as well as for the ease of access and retrieval from the off-site storage location, particularly in the event of a disaster.

d. Ensure the following are included in periodic backups and stored at the off-site storage facility:
   1) Source and object code for production programs.
   2) Master files and transaction files necessary to recreate the current master files.
   3) System and program documentation.
   4) Operating systems, utilities, and other environmental software.
   5) Other vital records.
   6) Encryption of data as prescribed by the data owners.

2. Responsibilities
   a. Chief Information Security Officer (CISO)/Departmental Information Security Officers (DISR)
      1) Identify which data and systems will be backed up and implement standard frequency of backup, based on the significance of the data and its frequency of change.
      2) Implement procedures for transferring the most current copy of backup media to a physically and environmentally secure off-site storage location.
      3) Ensure documented procedures exist for the recovery and restoration of information from backup media and that this documentation is also maintained at the offsite storage location.
      4) Monitor backup and recovery procedures and practices to ensure safety and recoverability of data and compliance with this guideline.
   b. System Administrators/Backup Operators
      1) Based on the determinations of the DISR, administrators shall regularly copy operating system software, application software, and production data to backup media and encrypt data as required by data owner. Transport or provide for the transportation and storage

of current backup media at an off-site storage location, ensuring that at least one current copy of backup media is stored off site at all times.
2) Develop and implement procedures for maintaining an inventory and tracking the location of backup media.
3) Document and implement procedures for the orderly restoration of information and its operating environment from backup media.
4) To ensure complete restoration of servers for disaster recovery, images of production servers may periodically be created and stored offsite.
5) Document detailed hardware specifications of servers.

c. End Users
1) End users should be directed to store their data on network server hard drives, rather than on their workstations.
2) Whenever critical data is stored on workstations, the same backup procedures apply as for network-housed data.

C. CHANGE MANAGEMENT

The purpose of this guideline is to mandate the use of communication and procedures that will minimize the risk and impact of changes to information systems throughout the County.

In a computer system environment, change management refers to a systematic approach to keeping track of the details of the system. For example, what operating system release is running on each computer and which fixes have been applied? Change management procedures facilitate the prompt and efficient handling of a Request for Change (RFC).

1. Change Management Roles
   a. The Information Technology Advisory Committee (ITAC) is generally composed of personnel who represent their department's information technology interests. The group assesses and advises on IT-related changes, and communicates findings with appropriate managers and stakeholders.
   b. A Change Manager oversees the change management process, from receipt and logging of an RFC through the implementation of change and notification of stakeholders.
   c. The Change Owner is a member of the team responsible for planning and implementing the change. This person, after having received an RFC, coordinates the development/procurement, testing, and implementation of the change, and works with the Change Initiator to ensure that the change meets the Initiator's requirements.
   d. The Change Initiator is any County employee who submits an RFC.

2. Change Prioritization

   Changes are prioritized according to their urgency and impact.

   a. Urgent changes need to be implemented as quickly as possible to correct a problem that is affecting mission-critical functions.
   b. High-priority changes correct a problem with mission-critical applications, processes or equipment.
   c. Medium-priority changes affect only a limited number of users.
   d. Low-priority changes can wait to be implemented during the next major release.

3. Change Outcome Notification
   a. As soon as possible following the change implementation process, the Change Manager (or other appropriate person, dependent upon the level of the change) shall provide outcome notification to all stakeholders, even if the implementation was not successful.
   b. During the change evaluation/monitoring phase, stakeholders should be kept up-to-date about the status of the assessment and any problems uncovered.
   c. For failed implementations, proper notification shall be provided that details the cause of failure, the next course of action, and how the stakeholders will be affected.
   d. Stakeholders must be informed if it is decided to not implement the change and evaluate other alternatives or cancel the change altogether. Stakeholders should also be informed of any follow-up activities that will be initiated.

4. Request For Change (RFC) Form

   A standard “Request for Change” form shall be utilized throughout the County for changes within the scope of this guideline.

REQUEST FOR CHANGE

Request ID #:		Date of Submission:	___/___/___	Priority (Circle One): Urgent High	Medium Low
Initiator Name / Phone:			Initiator's Department:		
Impact Assessment					
Description of Change:					
Business Reason:					
Technical Reason:					
Platforms Affected:					
Impact to Users:					
Backout / Recovery Plan Description:					
Impact Assessment Results:					
Training Requirements:					
Contact Information					
Change owner name:			Phone:		
Support staff 1 name:			Phone:		
Support staff 2 name:			Phone:		
Others:			Phone:		
			Phone:		
Other notes or comments:					

D. COMPUTER FORENSICS

The purpose of this guideline is to familiarize staff with the basics of computer forensics and define the minimum actions to support computer forensic investigations.

1. Overview of Computer Forensics

   Computer forensics shares all the laboratory practice requirements of traditional forensic science. The methods used and the results obtained may be presented in legal proceedings. The objective of computer forensics is to provide valid and reproducible results when examining computer-related evidence.

2. Forensic Elements
   a. Computer forensic science can rarely expect the same elements in each case.
   b. Operating systems, which define what a computer is and how it works, vary among manufacturers.
   c. Application programs are unique.
   d. Storage methods may be unique to both the device and the media.

3. Computer Evidence
   a. Computer evidence is represented by physical items such as chips, boards, computers, storage media, monitors, and printers. Additional and related evidence items to be gathered and used during forensic examination may include application and operating system documentation, passwords, notes and system configuration information.
   b. Computer evidence almost never exists in isolation. It is a product of the data stored, the application used to created and store it, and the computer system that directed these activities.

4. Extracting Evidence
   a. Proven laboratory practices are required by which examinations are planned, performed, monitored, recorded and reported to ensure the quality and integrity of the work product.
   b. Whenever possible, conduct the examination on copies of the original evidence, protecting the original evidence from accidental or unintentional damage or alteration.

      This principle is predicated on the fact that digital evidence can be duplicated bit for bit to create a copy that is true and accurate.

1) Each agency and examiner must make a decision as to the methodology for reliable copying to be used and ensure that it is true and accurate on a case-by-case basis.
2) Factors to be considered in copying include the amount of data, the method used to create it, and the media on which it resides.

5. Responsibilities
   a. End Users
      If inappropriate or criminal activity is suspected, contact your Departmental Information Security Representative (DISR) and your supervisor or manager.
   b. DISR and/or Management
      1) When notified by an end user of suspicious activity as noted above, physically isolate suspect equipment, disconnecting any network cable and preserving the On/Off state.
      2) Log your activities. This log is be key to a valid chain of evidence.
      3) Contact the Sheriff's Office's High-Tech Crimes Unit (925-313-2640) or alternately, the Main Investigations Desk (925-313-2600) for consultation and further instruction.
   c. Be advised that any forensic investigation may require the removal of not only the suspect equipment but data residing on production network servers. Such activity may impact the availability of services from this equipment.

E. DATA LINE

The purpose of this guideline is to define the acceptable usage of County data and facsimile lines. This guideline covers two distinct uses of analog and digital lines.

- Lines connected for the sole purpose of fax sending and receiving.
- Lines connected to desktop and laptop computers.

1. Security Risks

   There are two important scenarios that involve analog line misuse, which we attempt to guard against through this guideline.

   a. Outside Attacker
      An outside attacker who calls a set of analog line numbers hoping to connect to a computer with a modem attached to it. If the modem answers (most computers today are configured out of the box to auto-answer) from inside County premises, then there is the possibility of breaching County internal networks through that computer. At the very least, information held on that computer alone can be compromised.

b. Physical
The second scenario is the threat of anyone with physical access into a County facility being able to use a modem-equipped laptop or desktop computer. In this case, the intruder would be able to connect to the trusted networking of the County through the computer's Ethernet connection and then call out to an unmonitored site using the modem, with the ability to siphon County information to an unknown location.

2. Data Line Usage

The following applies to data line usage.

a. No lines will be installed for personal use.
b. Fax machines must be placed in a centralized administrative area and away from other computer equipment.
c. Desktop and laptop computers are not allowed to establish data or fax connections.

3. Waivers

Waivers may be granted on a case-by-case basis by the Departmental Information Security Representative (DISR). It is the responsibility of the DISR to maintain documentation on each waiver granted.

If approved, the requester must ensure compliance with the requirements listed below.

a. The data line is used solely as specified in the request.
b. Only persons authorized to use the line have access to it.
c. The line shall be physically disconnected from the computer when not in use.
d. The computer must be physically disconnected from the County's internal network when using the data line.
e. All downloaded material, prior to being introduced into County systems and networks, must have been scanned by an approved anti-virus utility, which has been kept current through regular updates.
f. Notify the DISR when the line will no longer be needed and may be deactivated.

F. DATABASE PASSWORDS

The purpose of this guideline is to define the minimum requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on the County's network.

1. Authentication

   Computer programs running on the County's network often require the use of one of the many internal database servers. To access one of these databases, a program must authenticate to the database by presenting acceptable credentials.

   The database privileges, that the credentials are meant to restrict, can be compromised when the credentials are improperly stored. In order to maintain the security of the County's internal databases, access by software programs must be granted only after authentication with credentials.

   The credentials used for this authentication must not reside in the main executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a Web server.

2. Authentication Requirements
   a. Storage of Database User Names and Passwords
      1) Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file must be properly secured.
      2) Database credentials may reside on the database server. In this case, a hash number identifying the credentials may be stored in the executing body of the program's code.
      3) Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.
      4) Database credentials may not reside in the documents tree of a Web server.
      5) Pass-through authentication must not allow access to the database based solely upon a remote user's authentication on the remote host.
      6) Passwords or pass phrases used to access a database must adhere to the County's Password Guideline.
   b. Retrieval of Database User Names and Passwords
      1) If stored in a file that is not source code, database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.

2) The area into which database credentials may be stored must be physically separate from the other areas of code (e.g., the credentials must be in a separate source file). The file that contains the credentials must contain no code other than the credentials (i.e., the user name and password) and any functions, routines, or methods that will be used to access the credentials.
3) For languages that execute from source code, the credentials' source file must not reside in the same read or executable file directory tree in which the executing body of code resides.

c. Access to Database User Names and Passwords
1) Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
2) Database passwords used by programs are system-level passwords as defined by the County's Password Guideline.
3) Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the Password guideline. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

G. DIAL-IN ACCESS

The purpose of this guideline is to protect the County's electronic information from being inadvertently compromised by authorized personnel using a dial-in connection. Dial-in access should be the method of last resort. Alternative methods shall be used to phase out any dial-in capabilities.

1. Dial-In Connection
a. County employees and authorized third parties (vendors, etc.) can use dial-in connections to gain access to the County network. Dial-in access should be strictly controlled, using one-time password authentication and dial-back. Modems should be disconnected or powered off at all times unless prior notice is given to allow a dial-in access connection.
b. It is the responsibility of employees with dial-in access privileges to ensure that a dial-in connection to the County is not used by non-employees to gain access to County information system resources.

Employees who are granted dial-in access privileges must remain constantly aware that dial-in connections between their location and the County are literal extensions of the County network and that they provide a potential path to the organization's most sensitive information. The employee and/or authorized third-party individual must take every reasonable measure to protect County assets. For information on cellular or other wireless access to the County network,

consult the Wireless Communications guideline.

Note: Dial-in accounts are considered "as needed" accounts. Account activity is monitored and if a dial-in account is not used for a period of two months, the account will expire and no longer function. If dial-in access is subsequently required, the individual must request a new account as described above.

c. Dial-in phone numbers are to be changed when employees no longer need the access, leave County service, or at least annually to ensure against war-dialing and possible malicious use.

H. DIGITAL SECURITY

The purpose of this guideline is to provide guidelines to limit the use of digital signatures to those created by a technology accepted for use by the County and proven to be valid for use by a public entity. In addition, this guideline provides direction to follow the California Government Code Section 16.5.

1. Digital Signature

   The digital signature is an electronic signature used to authenticate the identity of the sender of a message or the signer of a document and to guarantee that the document has not been changed by another party. Digital signatures are created and verified by cryptography, the enciphering and deciphering of messages, a method of transforming text in order to conceal its meaning.

2. Digital Signature Processes

   The use of digital signatures involves two processes:

   - One performed by the sender; and
   - The other by the receiver of the digital signature.

   Established public key cryptography should be used for the digital signature. Public key cryptography uses an algorithm that utilizes two different but mathematically related keys.

   One key is used for creating a digital signature or transforming the message into an unintelligible form. The second key is used for verifying a digital signature or returning the message to its original form.

   Computer equipment and software utilizing two such keys are often termed an asymmetric cryptosystem.

3. Digital Signature Validity

   The digital signature shall have the same validity as the use of a handwritten signature if and only if it has the following attributes.
   a. It is unique to the person using it.
   b. It is capable of verification.
   c. It is under the sole control of the person using it.
   d. It is linked to data in such a manner that if the data are changed, the digital signature is invalid.

4. Review of Digital Signature Requirements

   County digital signature requirements will be reviewed annually and upgraded as technology allows.

   The Chief Information Officer (CIO) and the Chief Information Security Officer (CISO) will direct the IT organization in the selection and/or approval of signature authorities.

   The use of digital signatures must include procedures for:

   a. Managing private key compromise.
   b. Insuring private key material is adequately secured.
   c. Long term storage and retrieval of keys in order to be able to validate signatures for the life of the resource signed.
   d. Revocation of signing keys.

I. EMPLOYEE BACKGROUND SCREENING

The purpose of this guideline is to safeguard the County's informational assets by preventing the hiring or continued employment of an ineligible person. To prevent the hiring or continued employment of an ineligible person, the County is committed to a thorough background screening of both criminal activity and fiscal responsibility. Eligibility for employment is based upon the requirements of the position being filled.

1. Background Screening of Employees

   This guideline consists of three components:
   - Standard fingerprint screening for criminal history through the State of California Department of Justice for all County employees.
   - Full credit/debt check; and
   - Full personal history background for those County employees considered to be working in the most sensitive areas.

2. General Screening
   a. Background screening will be required of all prospective employees who will be notified via a signed Offer of Employment letter.
   b. The original background screening must be completed before the employee hiring package is complete and before the employee's first day of work.
   c. This guideline may be invoked periodically to re-screen existing employees as needed.

3. Standard Fingerprint Screening
   a. Prospective or existing employees will be fingerprinted by agreement with the County Sheriff's Office or by another authorized entity. Contracts with private agencies are also available.
   b. The results are generally returned to the agency performing the fingerprinting within 10 working days.
   c. Generally, criminal history reports run by the Sheriff's Office on behalf of County provide only a pass/fail response, and do not provide the detailed findings to the agency requesting the history. The history detail is kept by the Sheriff's Office. This practice is based on existing statutes. If detail history is requested or needed, it would normally be advisable to have the screening performed by another authorized entity or a contracting agency.

4. Credit/Debt Check
   a. A standard credit check through one of several reputable credit clearing houses should suffice to provide a thumbnail of the prospective employee's fiscal responsibility.
   b. Often, the local Sheriff's Office or other County agency has bid and secured a resource for the credit check. Use of this contract can normally be expanded. Alternately and to maintain this information confidentially, the Sheriff's Office may also be a resource to perform this function on behalf of the County.

5. Personal History
   a. Performed optionally on request, the personal history can take on at least two characteristics:
      - Full law enforcement background check; or
      - The less-detailed version for use by non-law enforcement agencies looking for a bit more detail, but not to the extent of the volumes of information requested and produced for law enforcement.
   b. The standard Department of Justice form for law enforcement screening can be edited down to accommodate an abbreviated personal history report.

c. Note that a personal history screening, depending on the level of information processed, can take months of elapsed time and prove to be fairly costly.

J. EMPLOYEE TERMINATION

The purpose of this guideline is to define the methods to effectively limit and remove access for both voluntary and involuntary terminations within the County organization.

1. Termination of Employment with Contra Costa County - Any time an employee, consultant, or contractor is terminating his or her relationship with the County, swift action and methods are required to prevent the possibility of unauthorized access to County information assets by those who are no longer authorized to access those assets.

   Any employee being involuntarily terminated will be asked to leave the premises immediately upon notification, to prevent further access to computing resources. Voluntary terminations may be handled differently, depending on the judgment of the employee's supervisors, to enable the employee to complete work in progress or train a replacement.

   If the departing employee has authority to grant authorizations to others, these other authorizations will be reviewed and reassigned. All keys, badges, and other devices used to gain access to premises, information, or equipment will be retrieved from the departing employee by the employee's supervisor.

   Any special conditions to the termination (e.g., denial of the right to use certain information) will be reviewed with the departing employee during the employee "out-processing" procedure.

2. Voluntary Separation - Since terminations can be expected regularly, this will be accomplished by utilizing the *Employee Separation/Termination Checklist* for outgoing or transferring employees. This process will be included as part of the standard "out-processing," and put in place to ensure that system accounts are removed in a timely manner, and normally includes:
   a. Removal of access privileges, computer accounts, authentication tokens.
   b. The control of keys.
   c. The briefing on the continuing responsibilities for confidentiality and privacy.
   d. Return of property.
   e. Continued availability of data.

3. Involuntary Termination - In addition to the process identified for voluntary separation/termination, and given the potential for adverse consequences, the County will also ensure that involuntary terminations include:
   a. Terminating access as quickly as possible, preferably at the same time (or just before) the employee is notified of his/her dismissal.
   b. If applicable during the "notice of termination" period, assign the individual to a restricted area to function. This may be particularly true for employees capable of changing programs or modifying the system or applications.
   c. Any time termination involves a person in a position of trust such as a systems administrator, the County will have a replacement administrator chosen and ready to assume their duties immediately.

4. Termination Process - In the event that an employee, consultant, or contractor is terminating his or her relationship with the County, the employee's immediate management is responsible for ensuring all property in the custody of the employee is returned, that the IT InfoSec team is given notification by utilization of the *Employee Termination/Separation Checklist* in order to revoke all computer access rights for that individual, that administrators handling the computer accounts used by the employee, consultant, or contractor are notified, and that all other work-related privileges of the employee are terminated.

   Upon notification of an employee's termination from employment at the County, the following will be done:

   a. The department manager or designee will notify the HR and IT InfoSec staffs, and complete the Employee Termination/Separation Checklist.
   b. The department manager or designee will notify those departments in which the employee, consultant, or contractor had access through keys, tokens, or access cards so that all access privileges can be deactivated.
   c. HR will begin "out processing."
   d. A copy of the Employee Termination/Separation Checklist will be forwarded to the IT InfoSec team. Following the guidelines outlined in the checklist and the separation date, IT InfoSec will:
      1) Ensure employee's name has been removed from any internal system access lists, authentication server lists, firewall lists, etc.
      2) Terminate employee's access to network, standalone applications, email (internal and external), etc.
      3) If the employee had access to any network passwords (to include routers, modems, firewalls, etc.) change them at this time
      4) Terminate employee's access to unique County computers, servers, and systems, etc. Change passwords if necessary
      5) Terminate remote access account(s) (if applicable)
      6) Assign access rights over the user's files and directories

7) Re-route email to the appropriate individual identified by department management
8) When applicable, perform a general security scan of the system(s) for any unknown back doors, etc.

e. On or near the last day of employment, the department manager or designee will meet with the employee to receive identification materials, keys, tokens or access cards used to permit access to County facilities. In the event the employee has County equipment off-site (home office privileges with laptop computer), this equipment will be turned over to the department manager or designee and forwarded to the IT department during the last scheduled day of employment. The employee will be asked to read and sign a non-disclosure agreement intended to protect confidential and private information.
f. Documentation of items received and a copy of the Employee termination/separation Checklist will be kept in the employee's permanent record of employment with the County.
g. All user-IDs identified as inactive will automatically have the associated privileges revoked after a thirty (30) day period.
h. All inactive accounts will be removed from County systems after a forty-five (45) day period.
i. All department managers will receive a monthly list of employees who have approved security codes to determine if there are any individuals who are no longer employees of the County. This list will be reviewed, updated, and returned to the IT department InfoSec team within one week of receipt.

EMPLOYEE SEPARATION/TERMINATION CHECKLIST

Employee Name:		Employee ID No.:	
		Department:	
Date Hired:		Separation Date:	
Department Manager Signature			
The person who will receive access rights over the user's files and directories:	Name:		
	User ID:		

Department Manager:

(All custody forms should be included with this separation/termination checklist.)

[ ] Keys (office, building, other)
[ ] Badge/ID (office, building, other)
[ ] Card keys (office, building, other)
[ ] Keyless entry account deleted
[ ] Company guidelines and/or manual(s)
[ ] Departmental/company-issued IT equipment
[ ] Tools/equipment/safety equipment
[ ] Purchasing card(s)
[ ] Telephone calling card/account
[ ] If departmental purchaser, contact suppliers and vendors to cancel employee as authorized purchaser
[ ] _____

INFORMATION TECHNOLOGY DEPARTMENT:

[ ] Network access account (network, mainframe, servers, etc.)
[ ] E-mail account
Should e-mail be rerouted? If so: User ID: _____
[ ] Computer and/or laptop
[ ] Printer (laser, inkjet, all-in-one)
[ ] Cell phone and accessories
[ ] PDA
[ ] Pager
[ ] Telephone access [ ] Voice mail
[ ] Distribution list
[ ] VPN connection access
[ ] Company-provided dial-up account access
[ ] Cancel specific software access (accounting software, HR software, etc.)
[ ] If IT equipment authorized purchaser, contact suppliers and vendors to cancel employee as authorized purchaser

K. ENCRYPTION GUIDELINES

The purpose of this guideline is to provide guidelines that limit the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this guideline provides direction to ensure that federal regulations are followed and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

1. Encryption Algorithms - Proven, standard algorithms should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. Symmetric cryptosystem key lengths must be at least 56 bits. Asymmetric cryptosystem keys must be of a length that yields equivalent strength. The County's key length requirements will be reviewed annually and upgraded as technology allows.

   The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by security administration. The export of encryption technologies is restricted by the U.S. government.

L. EXTRANET GUIDELINES

The purpose of this guideline is to ensure that extranet access to County informational assets is secure and used for County business only.

1. Pre-Requisites
   a. Security Review
      All new extranet connectivity requests will go through a security review by the Department Information Security Representative (DISR) to ensure that all access matches the business requirements in the best possible way and that the principle of least privilege is followed.
   b. Third-Party Connection Agreement
      All new connection requests between third parties and County require that the third-party and County representatives agree to and sign a Third-Party Agreement which ensures compliance with all County policies. The technologies used for connectivity must meet County standards including, at a minimum, access and authentication protocols and appropriate audit trails.

      This agreement must be signed by a senior manager in the County as well as a representative from the third party who is legally empowered to sign on behalf of the third party. The signed document is to be kept on file with the relevant extranet group (department).

c. Point of Contact (POC)
The sponsoring organization/department must designate a person to be the POC for the extranet connection. The POC has the following roles:
- Can be the department Information Security Representative.
- Acts on behalf of the sponsoring organization.
- Is responsible for those portions of this guideline and the Third-Party Agreement that pertain to it.

In the event that the POC changes the relevant extranet organization must be promptly informed.

2. Connectivity and Access
   a. Establishing Connectivity
   All connectivity established must be based on the principle of least privilege in accordance with the approved business requirements and security best practices. In no case will the County rely on the third party to protect the County network or resources.
   b. Modifying or Changing Connectivity and Access
   All changes in access must be accompanied by a valid business justification and are subject to security review. Changes are to be implemented via the approved change management process. The sponsoring organization is responsible for notifying the appropriate department when there is a material changes in their originally provided information so that security and connectivity evolve accordingly.
   c. Terminating Access
   When access is no longer required, the sponsoring organization within the County must notify the extranet team responsible for that connectivity, which will then terminate the access. This may mean a modification of existing permissions up to terminating the circuit, as appropriate.

   Annually, existing connections are to be removed to ensure that they still needed and that the access provided meets the needs of the connection. Connections that are found to be no longer of value and/or are no longer being used to conduct County business will be terminated immediately.

   Should a security incident or a finding that a circuit has been deprecated and is no longer being used to conduct County business necessitates a modification of existing permissions or termination of connectivity, the appropriate department will notify the POC or the sponsoring organization of the change prior to taking any action.

M. INFORMATION ASSETS

The purpose of this guideline is to define procedures and responsibilities for managing information assets.

1. Information Asset Management

   All County personnel and, in particular, County I.T. organizations will adopt measures to protect the County's information assets. Information assets include, but are not limited to:

   a. Computer storage media, including tapes, disks, diskettes, CD-ROMs, and similar media
   b. Computers, modems, and other hardware attachments
   c. Fax equipment
   d. Local area networks (LANs)
   e. Pagers
   f. Printers
   g. Radio equipment, PDAs, and other handheld devices
   h. Scanners
   i. Telecommunications networks
   j. Telephones
   k. Terminals and workstations
   l. Wide area networks (WANs)

2. Physical Sites Housing Information Assets

   Personnel will ensure the safeguarding of information assets by establishing procedures and assigning responsibilities for use of information assets. These include the following:

   a. Safeguard all information assets.
   b. Establish information asset usage privileges and access in accordance with the IT Security Administration guideline.
   c. Manage the replacement of older information assets and purchase of new information assets.
   d. Allow only authorized personnel access to sensitive information assets. Examples include:
      1) Persons with systems and technology knowledge and skills who are responsible for operating an information asset.
      2) Operating system software and related documentation.
      3) Application software and related documentation.
      4) Information produced, delivered, or maintained by another information asset.

5) Licenses, contracts, and other records relating to information assets.

3. All Users
   a. Obtain authorization from appropriate management to use an information asset.
   b. Protect the accuracy, integrity, and confidentiality of information that has been produced, delivered, or maintained by another information asset.
   c. Report misuse, damage, or theft of an information asset immediately to the next highest level of management or directly to the Departmental Information Security Officer (DISR).

4. Information Technology
   a. Assist in the orderly and systematic replacement of older technology as necessary.
   b. Preserve the integrity of the control environment in user departments as equipment is replaced.

5. Procedure Components

   Standard procedures for protecting various forms of sensitive information should be developed and implemented. The following components should be identified.

   a. The “creator” and/or “owner” of the information and the individual or group responsible for ensuring its security.
   b. The custodians who have “authorized possession” of the asset e.g., the data processing (DP) function or a service center.
   c. Users of the information i.e., those who have access to the asset.
   d. The method of securing the information, including specific procedures that relate to the class of information being protected.
   e. Retention guidelines for the information.
   f. Methods of safely storing the information.
   g. Methods of disposal or disposition of the information.

N. <u>INFORMATION CLASSIFICATION</u>

This guideline defines how information is to be classified based upon its relative sensitivity and to help employees determine under what conditions information may be disclosed to non-employees.

All information is categorized into two main classifications: Public and Sensitive.

Questions about the proper classification of a specific piece of information should be addressed to one's manager.

1. Public Information
   a. Information that is available to anyone who asks based on legislative mandate, such as County, State, and/or Federal regulations or declared to be public by someone within "the County with the authority to do so". This information is to be provided via due process in order to ensure that the information is in fact public and that the cost for providing the information is appropriately recovered. Public available information still requires access controls for authorized changes.
   b. Unless regulations demand otherwise, any information that is marked "Draft", "Confidential" or "Sensitive" is not public by definition. If information is not marked or otherwise classified, County information is presumed to be sensitive unless expressly determined to be County public information by a County employee with authority to do so.
   c. Unless you have the authority to interpret what is public information, verify requests through your manager.
   d. For more information see the California Public Records Act contained within California Government Code 6254.9.

2. Sensitive Information
   a. Sensitive information includes the following:
      - Restricted Data
      - Private or Confidential Data
      - Protected Data
      - Intellectual Property
   b. The Information Owner is the classification authority. It is the responsibility of the Information Custodian to apply appropriate measures to protect all information assets so classified by the owner of that information.
   c. Listed below are guidelines for classifying information.
      1) Non-Sensitive Information – This information is considered public information and has been declared public by the California Public Records Act. For guidance on releasing public information beyond the scope of one's immediately defined work responsibilities, refer to your management.
      2) Sensitive Information – Examples include personal, medical records or financial information on employees, constituents, citizens, customers, business partners, or anyone else that has not been previously defined in law to be a public record. Sensitive information may also include any other information that could enable an individual to commit identity theft when so defined in law or policy.

Other sensitive information includes critical infrastructure schematics or infrastructure protection plans, including buildings, vehicles, telecommunication and systems. Information that is covered by non-disclosure agreements or intellectual property practices is considered sensitive information.

Sensitive information can be broken down into other classifications:

- Restricted
- Private or Confidential
- Protected
- Intellectual Property

3) Restricted Information - Examples of restricted information include CLETS, Coroner, District Attorney, Public Defender and Protected Health Information (PHI), system documentation, and details about the operating environment hosting restricted information. Information of this nature is sensitive and could have immediate detrimental effects if released to the wrong individuals. Specifically, restricted information could expose individuals to danger, suspend large segments of business operations, or cause extensive damage to resources.

   Only County personnel designated in writing and approved by the information owner are authorized access to restricted information. Access approval processes are developed for each restricted system.

   The information owner retains classification authority, access control, and distribution control responsibilities. The owner Department designates restricted data and systems by letter to the CIO or IT Director. Restricted data may also be contained in the following elements of restricted systems:
   a) Computer readable files
   b) Reports and Printouts
   c) Terminal and Monitor displays
   d) Program Source and Object code
   e) Systems and Program documentation
   f) User documentation
4) Private or Confidential Data - Some data collected and maintained by the County are protected from public disclosure through various privacy and confidentiality statutes, and thus are not available under existing public information laws. Examples of private or confidential information include:
   a) Passwords
   b) Personal medical condition or related information
   c) SSN

d) Personal or family information
e) Family names
f) Ages
g) Personal or business partner financial and banking data, including credit cards, bank routing numbers and bank account information
h) Personal information provided by constituents in the course of delivering any public health or social service (name, address, phone, SSN, family names, personal historical detail)
i) County financial data not deemed public by the Public Records Act
j) Employee performance reviews, discipline reports and other personnel data
k) Information related to in-progress legal proceedings
l) The combination of a logical address, User ID, and password
m) County-owned or third-party Intellectual Property

Only County personnel with a designated need-to-know are authorized access to private or confidential information. The information owner retains classification authority, but County managers are authorized to approve or disapprove both access and distribution requests. When in doubt, however, managers must always obtain Department information owner consent before granting access or releasing information.

5) Protected Data - This is information generated in the normal course of managing County operations that may be a public record under the State of California Public Records Act. However, if made available by publishing in a public medium would create a potential physical threat or potential disruption to county operations. Examples of protected information include:
a) Telecommunications and cabling schematics
b) Disaster Recovery Plans
c) Operational Recovery Plans
d) Network schematics
e) Physical facility schematics
f) Preliminary reorganization plans
g) Detailed information about ongoing projects
h) Time sensitive information
i) Risk assessments
j) System controls

Only County personnel with a designated need-to-know are given authorized access to protected information. The information owner retains classification authority, but County managers are authorized to approve or disapprove both access and distribution requests.

When in doubt managers must always obtain Department information owner consent before granting access or releasing protected information.

6) Intellectual Property - Without specific written exceptions, all programs and documentation generated or provided by employees consultants, or contractors for the benefit of the County are the property of the County. The County has legal ownership and therefore maintains exclusive rights to patents, copyrights, inventions, or other intellectual property developed by employees, consultants, or contractors for use on County systems. This includes intellectual property stored on County computer and network systems as well as all messages transmitted via these systems. County software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-County party for any purposes other than County business purposes.

   Registered software purchased from a non-County source is considered third-party intellectual property. Ownership and limitations on use are established by the registered owners' licensing agreements.

3. Information Classification - Information ownership is the direct responsibility of user departments. Department Heads and/or designee are responsible for being knowledgeable about confidentiality and privacy laws specific to their Department's functions. Department Heads and/or designees are responsible for all aspects of the classification, use, distribution and protection of County information within and outside of their respective departments. This responsibility includes determining the level of access to be granted to a user. Information owners are responsible for coordinating with their information custodians to assure that facility security needs of sensitive information are met.

4. Evaluating the Sensitivity Level

   To assist in evaluating the sensitivity of information, consider the following criteria:
   - Availability
   - Financial value
   - Timeliness
   - Purpose

5. Declassifying or Reclassifying Information
   a. Only the Information Owner may downgrade or declassify information. Downgrading is the process, as an example, of reclassifying information from “Restricted” to “Confidential.” Declassifying is the process of reclassifying information from “Confidential” to “Unclassified” or “Public.”
   b. The sensitivity guidelines below provide details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as confidential County information in each column may necessitate more or less stringent measures of protection, depending upon the circumstances and the nature of the confidential County information in question.
   c. A given sensitivity designation is assumed to stay in effect until explicitly changed by the information owner or someone in the County with the authority to do so.

6. Minimal Sensitivity

   General organization information; some personnel and some general technical information.

   a. Labeling
      1) Marking or labeling is at the discretion of the owner or custodian of the information.
      2) If marking is desired, the words “County <Department Name> Sensitive” may be written or designated in a conspicuous place on or in the information in question.
      3) Other labels that may be used the discretion of your individual business unit or department.
   b. Access
      County employees and non-employees with a business need to know.
   c. Distribution within County
      1) Standard interoffice mail
      2) Approved electronic mail
      3) Electronic file transmission methods
   d. Distribution Outside of the County Internal Mail
      - U.S. mail and other approved carriers.
   e. Electronic Distribution
      - Must be sent to approved recipients.
   f. Storage
      1) Keep from view of unauthorized people.
      2) Should not be stored or displayed on machines without physical and software access controls.
      3) Protect information from loss.
      4) Any medium for backup/recovery should have the same or better access and security controls as the original data.

5) Electronic information should have individual access controls where possible and appropriate.
6) Information should not be stored in a given location any longer than the business function or regulation requires e.g., downloading files to telecommuting machines, laptops, PDA's etc.
7) Equipment that is no longer under the physical control of the County must have information expunged/cleared prior to transferring control to an outside agency e.g., surplus, sending equipment out for repair, loaning equipment, etc.

g. Disposal/Destruction
1) Shred outdated paper information.
2) Electronic data should be expunged/cleared.
3) Reliably erase or physically destroy media.

7. More Sensitive
a. Financial, technical, and most personnel information.
b. Labeling - Marking must indicate "Confidential" rather than "Sensitive."
c. Access - A signed nondisclosure agreement shall exist.
d. Electronic Distribution - Transmission must be via a private link or securely encrypted.
e. Storage - Information transferred to any portable media must be encrypted.

8. Most Sensitive
a. Operational, personnel, financial, source code, and technical information such as configurations, connectivity diagrams, patch procedures. Any information that could be used to impersonate a person or a process or lead to unauthorized access or modification of information.
b. Labeling - Marking must indicate "Classified" rather than "Confidential."
c. Distribution within the County - Delivered direct requires signature; envelopes stamped classified.
d. Distribution Outside of the County Internal Mail - Delivered direct requires signature required and approved carriers.
e. Electronic Distribution - Transmission must be securely encrypted.
f. Storage - Individual access controls are required for all forms of storage.

O. INFORMATION TECHNOLOGY STEERING COMMITTEE

The purpose of this guideline is to encourage cooperation, collaboration, and consensus among County departments with regard to information technology through the Information Technology Steering Committee (ITSC).

1. Role of ITSC

   The ITSC will evaluate IT opportunities from a countywide perspective for fit within the overall business strategy and mission of the County, and make IT recommendations to the County Administrative Office (CAO).

   The ITSC identifies the priority and estimated funding levels of new IT initiatives to be undertaken jointly by County departments. The ITSC will consider initiatives from the Information Technology Advisory and Information Security Advisory Committees (ITAC and ISAC) for acceptance and sponsorship.

2. ITSC Responsibilities
   a. Governance
      1) Recommend the alignment of central IT services, standards, and resources with County business needs.
      2) Recommend the demarcation of centralized and decentralized IT services.
      3) Utilize the advice of the ITAC and ISAC to evaluate and recommend IT architecture, infrastructure, infrastructure security, and standards as a method to manage the total cost of ownership (TCO) component of IT investments.
      4) Provide a forum for stakeholders with a common set of business automation issues or opportunities to participate in the setting of IT priorities.
      5) Develop an annual IT plan with clear priorities to guide the overall IT budgeting process.
      6) Remand to departments day-to-day operational IT issues, technological decisions, and IT personnel matters.
   b. Evaluation Process
      1) The ITSC will evaluate for endorsement recommendations of the subcommittees.
      2) Monitor major IT project activity countywide and advise the Chief Information Officer (CIO) and CAO as needed.
      3) Review and revise IT evaluation criteria for use countywide in the development of requests for new IT initiatives that will come before the ITSC.
      4) Provide resolution of escalated prioritization issues.
   c. Evaluation Criteria for IT Initiatives
      1) The definition and scope of the proposed IT project or initiative.
      2) Proposed outcomes of the IT initiative.
      3) Beneficiaries of the implementation of the IT initiative or project.
      4) The expected benefits defined in financial terms or by other metrics.
      5) The estimated one-time and on-going costs.

6) The estimated duration of the project.
7) Potential or proposed source of funds (one-time and sustaining).

d. Meetings
   1) The ITSC will meet as needed.
   2) Agendas will be published prior to and will be used to manage the meeting time effectively.
   3) Meeting minutes will be published in a timely manner.
   4) The status of projects authorized via the ITSC will be published on a regular basis.

P. INSURANCE GUIDELINE

The purpose of this guideline is to establish County guidelines for periodic risk reviews for the purpose of purchasing and modifying insurance policies.

This guideline applies to any County information system that is covered by a commercial insurance policy and to the staff responsible for supporting the respective system.

1. Risk Analysis to Identify Insurance Needs
   a. Risk analysis will be performed to identify assets and identify County insurance needs. Procedures for recovering or replacing assets will be documented. Procedures will be established to ensure all relevant documentation is kept current and accurate as assets are added or removed.
   b. All insured equipment shall be inventoried and documented.
   c. Store insurance policies, procedures and documented information in a secure location.
   d. Include copies of insurance policies, procedures and information offsite with the disaster recovery plan.

Q. INTERNET DMZ EQUIPMENT

The purpose of this guideline is to define standards to be met by all equipment, owned and/or operated by the County, located outside the County's Internet firewalls. This guideline applies to all equipment or devices deployed in a DMZ owned and/or operated by the County (including hosts, routers, switches, etc.) and to the persons supporting said equipment.

These standards are designed to minimize the potential exposure to the County from the loss of sensitive or confidential data, intellectual property, damage to public image, etc.

1. Ownership and Responsibilities

   Equipment and applications within the scope of this guideline must be administered by support staff approved by the DISR for DMZ system, application, and/or network management.

   Support staff will monitor the equipment in the DMZ and have the right to disable without delay equipment suspected of negatively impacting the security of the network. Additionally, they will be responsible for the following:

   a. Documentation of the Equipment
      At a minimum, the following information is required:
      1) Host contacts and location.
      2) Hardware and operating system/version.
      3) Main functions and applications.
   b. Management of Privileged Passwords
      1) Assurance that hosts in the DMZ use appropriate domain name servers.
      2) Provision of access to equipment and system logs per the County Audit guideline.
      3) Changes to existing equipment and deployment of new equipment in accordance with the County's Change Management guideline.
      4) Approval of hardware, operating systems, services and applications as part of the pre-deployment review phase.
   c. Secure Configuration Requirements
      All equipment must be configured according to the configuration parameters below, unless a written waiver is obtained from the Departmental Information Security Representative (DISR) and the Chief Information Security Officer (CISO).
      1) Operating system configuration must be done according to secure host and router installation and configuration standards approved by the County Information Technology department.
      2) All patches/hot-fixes recommended by the equipment vendor and County Wide Area Network (WAN) group must be installed. This applies to all services installed, even though those services may be temporarily or permanently disabled. Administrative owner groups must have processes in place to stay current on appropriate patches/hot fixes.
      3) Services and applications not serving business requirements must be disabled.
      4) Trust relationships between systems may only be introduced according to business requirements, must be documented, and must be approved by the WAN group.

5) Services and applications not for general access must be restricted by access control lists.
6) Insecure services or protocols, as determined by the WAN group, must be replaced with more secure equivalents whenever such exist.
7) Remote administration from outside the County WAN must be performed over secure channels as governed by the County's *VPN guideline.*
8) All host content updates must occur over secure channels.
9) Security-related events must be logged and audit trails saved to WAN group-approved logs. Such events include (but are not limited to) the following:
   - User login failures.
   - Failure to obtain privileged access.
   - Access guideline violations.

2. Change Control Requirements

   All new installations and changes to the configuration of existing equipment and applications must follow the following policies/procedures.

   a. New installations and configuration changes must be approved by the WAN group.
   b. The WAN group will perform system/application audits prior to the deployment of new services.

3. Equipment Outsourced to External Service Providers

   Responsibility for the security of equipment deployed by external service providers must be clarified in the contract with the service provider, with security contacts and escalation procedures documented.

R. INFORMATION TECHNOLOGY SECURITY ADMINISTRATION

The purpose of this guideline is to provide Information Technology (IT) security administration guidelines for the development of procedures and defines the responsibilities for management, the County's IT security administrators, all users, and IT services.

1. I.T. Security Administration

   The security of any computer system involves safeguards for the hardware, the software, and all data in the system. It also involves the prevention of unauthorized access and alteration of data. Each individual user has responsibilities related to maintaining security over the County's information assets.

IT Security administration responsibilities should be segregated from systems development, computer operations, and systems programming functions.

2. Responsibilities
   a. County Management
      1) Assign an IT security administrator(s) who is responsible for controlling and monitoring online or electronic access to information assets.
      2) Involve IT personnel in the evaluation of security and access controls in any new hardware and software under consideration.
   b. I.T. Security Administrators
      1) Protecting the automated resources of the County from unauthorized destruction, modification, use, and disclosure.
      2) Develop IT security policies as needed and review existing policies for effectiveness.
      3) Enforce security standards, ensure compliance with established policies, procedures, and standards, and propose sanctions for noncompliance.
      4) Establish security guidelines for user profiles.
      5) Review system logs and security violation reports.
      6) Monitor access to systems or information outside the normal patterns or needs of a user or specific workstation.
      7) Report potential security breaches, as appropriate, to department heads and/or public information officers. Monitor and document security violations.
      8) Provide suggestions and recommendations to IT on security-related matters.
   c. All Users
      Report suspicious systems activity that may indicate that files or programs have been tampered with to the Security Administrator and Department Manager.
   d. Department of Information Technology Services
      1) Maintain security over the County's network infrastructure to ensure that one department does not have unauthorized access to another department's information.
      2) Review security and access controls in new software being considered for acquisition by multiple departments.

S. MASS STORAGE DECOMMISSIONING

The purpose of this guideline is to establish requirements regarding the disposal of mass storage devices in order to meet confidentiality and privacy requirements. The overall goal of this guideline is to protect the County and the public from unauthorized release of data.

1. Storage Media Disposal - This guideline requires that all storage media (including magnetic, optical and embedded memory systems) be erased or destroyed before any transfer, disposal, or surplus occurs.

2. Tracking Requirements - A database or other method of tracking decommissioned equipment should be implemented for all capital assets and other media as deemed necessary based upon the sensitivity of contained data.

3. Procedures - Departmental decommissioning procedures should be developed that implement the highest level of data destruction. Storage devices will be destroyed, or wiped as per Department of Defense (DoD) regulation 5220.22-M.

T. MONITORING

The purpose of this guideline is to assert the County's right to monitor electronic records e.g., e-mail/Internet in order to protect County assets from being used for improper purposes.

1. Employee Access for Business Use - Employees of the County are provided access to company telephones, voicemail, computers, e-mail, networks, Internet systems, fax machines, equipment, and other furnishings (including desks, drawers, and cabinets) for the purpose of performing their job-related duties on behalf of the County.

   The County reserves the right of immediate access to any County-owned equipment and storage upon reasonable concern that the employee entrusted with such equipment and/or storage is using it for an improper purpose.

   The County also reserves the right to conduct random reviews of employees' computers, e-mail, and voicemail systems for the purpose of ensuring that this equipment is being used for the business purposes for which it is intended and not for any improper purpose.

2. Disclosure of Electronic Records - County eMail/Internet records are subject to disclosure to law enforcement or government officials or to other third parties through subpoena or other processes. Consequently, you should always ensure that the business information contained in these messages is accurate, appropriate, and lawful.

3. Privacy - County employees may not expect or assert a right of privacy in connection with any County-owned assets. E-mail, voicemail messages and Internet records are to be treated like shared paper files, with the

expectation that anything in them is available for review by authorized County representatives.

The County reserves the right to monitor employees' incoming and outgoing phone calls on its business phone lines on a random basis for training, quality assurance, public service, and disciplinary purposes to determine whether excessive personal phone calls are occurring during business hours.

If monitoring occurs, and the County representative determines that the phone call is personal, he or she will immediately hang up the phone. Personal phone calls on County time are prohibited, except in case of emergency. Employees may make personal calls during breaks and other non-work time.

U. PATCH MANAGEMENT

The purpose of this guideline is to provide guidelines for the testing and implementation of software patches to County information systems.

1. Patch Management

   Patch management is a continual process whereby the goal is to minimize the time between threat identification and elimination. It is best implemented through a two-pronged approach:
   - Response to an announced threat; and
   - Preventive maintenance.

2. Response to an Announced Threat
   a. An announcement occurs stating the vulnerabilities. Specifically, your system has been compromised by a virus or other vulnerability.
   b. Locate and/or identify corrective action, as the greatest number of attacks are from known vulnerabilities.
   c. Ensure that vendor-supplied patches are applied. Apply and test the patch in a test environment as close as possible, in both hardware and software, to the production environment.
   d. Apply the patches to the production environment.
   e. Monitor the patched environment for new anomalies that may now be present in the patched software.

3. Preventive Maintenance

   Regularly assess, triage and resolve various threat levels through the use of the following:
   a) Automated detection software.
   b) Operating system vendor announcements.

c) Anti-virus vendor updates and postings.
d) Notifications or postings regarding commercial, off-the-shelf (COTS) applications.
e) Other trusted Web posting sites.

V. SECURITY PERIMETER & SUPPORTING ARCHITECTURE

The purpose of this guideline is to define the Security Perimeter and its supporting architecture. This guideline also establishes the core strategies, essential policies and operational requirements regarding the management and maintenance of the Security Perimeter and its supporting architecture.

1. Security Perimeter

   The Security Perimeter is defined as all resources, systems, connectivity, and services responsible for enabling and maintaining connectivity between this organization, its business partners, and all other external-to-organization resources or services. It represents the "managed point of entry/exit" to County infrastructure resources. The Security Perimeter includes, but is not limited to:

   - Firewalls
   - Intrusion Detection Systems (IDS)
   - Demilitarized Zones (DMZ's)
   - Remote Connectivity Resources; and
   - Network Architecture Resources providing connectivity for the environment.

2. Security Perimeter Strategies

   Essential to the Security Perimeter is the adoption of core Security Perimeter strategies. These core strategies are:

   a. Deny All; That which is not expressly permitted is denied - Services as a general rule are denied unless expressly defined. The application of a "deny all" strategy suggests that only the required (and thereby configured) services will be available. All other unused services are denied.
   b. The Principle of Least Privilege - The principle of least privilege states that an object (host, service, resource, subnet, etc.) should have the minimum privileges necessary to perform its assigned task and no more.
   c. Minimize Publication of Information - The best business practice and strategy is to minimize the amount of internal network resource information that is disclosed to trusted and non-trusted entities.

d. Single Entry/Exit - The best business practice and strategy is to have a single point of entry to the Wide Area Network or Intranet. (While this may not be achieved physically, it is critical that security standards are applied logically and uniformly across the defined Security Perimeter).
e. Principle of Accountability and Responsibility - To be accountable for security, one must be responsible for the resources that maintain it.

In accordance with these strategies the following guideline statements apply to the key areas and functions of the Security Perimeter. In all statements where the "County Authority" (CA) is mentioned, depending on the County reporting structure, this can be the CIO, CISO, CTO, CEO or COO and implies the CA or their designee(s).

3. Security Perimeter Authority

The County Authority is the root authority for the Security Perimeter. All resources, systems, connectivity, and/or services must be evaluated and approved by the CA before implementation can occur.

In this role the CA may take any action deemed necessary to ensure the security of County resources. This includes but is not limited to:

- Termination/Shutdown of Connectivity
- Termination/Shutdown of Services
- Termination/Shutdown of Resources
- Termination/Shutdown of Systems
- Revocation of Administrative Privileges

All actions taken by the CA are subject to review and/or appeal by the appropriate County governance structure.

4. Auditing and Vulnerability Assessment

The Security Perimeter provides an initial and critical function in maintaining the security of County infrastructure resources. To accomplish this function, several periodic and routine tasks are required.

a. Internal Auditing - Regular auditing which at a minimum, must include consideration of defined configuration parameters, enabled services, permitted connectivity, current administrative practices, and adequacy of the deployed security measures.
b. External Auditing - Periodic auditing, which assesses the efficiency and accuracy of internal auditing, is performed by individuals, groups, or third parties not involved with the Security Perimeter.
c. Vulnerability Assessment - The regular execution of vulnerability identification measures, which includes internal and external County

assessments, and may include assessments by bonded external third parties.

d. External Connectivity - External connectivity refers to all connectivity to or from the County. This commonly includes all business-to-business or Extranet connectivity, Internet and Internet-related connectivity. With respect to the Security Perimeter the following external connectivity guideline statements apply:
    1) Any external connection to or from the County Wide Area Network must come through the Security Perimeter's managed point of entry
    2) Only authorized outbound services will be initiated from internal County hosts to external-to-County hosts as approved by the CA
    3) The CA will approve inbound services on a case by case basis
    4) Extranet partners connecting to County resources cannot use the County as a conduit for connectivity to each other
    5) Any entity connecting to the County shall sign all necessary security and confidentiality agreements.

5. Logging

   Logging is a critical discipline to maintenance of security systems and serves multiple functions. With respect to the Security Perimeter the following logging guideline statements apply.

   a. All changes to the Security Perimeter, including but not limited to configuration parameters, enabled services, and permitted connectivity, must be logged. These change logs must be secured.
   b. The integrity of system logs must be protected with checksums, digital signatures, encryption, and/or similar measures.
   c. Removal or recording of system logs from their associated systems must be performed in a secure manner to ensure admissibility in court.
   d. System logs must be reviewed to ensure that the Security Perimeter is operating in a secure manner and to detect anomalous activity.
   e. Any anomalous activity indicating or suspected of indicating unauthorized usage or access must also be documented according to system procedures.

6. Remote Access

   Remote Access refers to remote access connectivity, such as dial-up networking and/or Virtual Private Networking (VPN), utilized to gain privileged access to County Infrastructure systems. The following guideline statements apply.

   a. In accordance with external connectivity guideline, all remote access connections must come through the Security Perimeter.

b. Resources used to remotely connect to County networks and resources must adhere to the adopted security requirements for remote resources (virus protection, personal firewalls, etc).
c. Remote access sessions will be monitored and logged and employ session time limits (active idle).
d. Remote access sessions utilizing the Internet as the means of connectivity must be encrypted in accordance with standards approved by the CA.
e. Remote access sessions connecting to County networks and resources must, in all instances possible, involve extended user authentication (single to multifactor authentication) measures approved by the CA.

7. Information Sharing and Publication

In accordance with the strategy of minimizing the publication of information, the following statements apply.

a. All Security Perimeter administrators, vendors and/or other third parties must sign appropriate Non Disclosure or Confidentiality Agreements.
b. All architecture and service related information with regard to the Security Perimeter must be secured.
c. Only information deemed appropriate by the CA may be shared openly.
d. Where appropriate, resources of the Security Perimeter must be configured in such a way as not to divulge their function and/or location.
e. Where capable and appropriate, resources must display warning banners that meet legal requirements for prosecution as approved by the CA.

8. Multi-Layer Security

Multi-layer security provides an increased deterrent to unauthorized use and/or access. In accordance with the Security Perimeter architecture design and architecture components as approved by the CA, the architecture should include all of the following.

a. Deployment of dedicated firewall technologies.
b. Deployment of demilitarized zones (DMZs) for resource hosting (i.e., Internet/Extranet accessible resources) and access filtering.
c. Deployment of Network Intrusion Detection Systems (NIDS) on all capable segments (Protocol Anomaly Detection (PAD) and signature detection capable).
d. Deployment of Host Intrusion Detection Systems (HIDS) on all capable hosts.

e. Virus screening resources on all necessary entry points.

9. Perimeter Resource Security

   Access to resources within the Security Perimeter must be provided in a manner that adheres to the Strategy of Least Privilege and the Principle of Accountability and Responsibility. To this end, the following statements apply.

   a. All resources, systems, connectivity devices, and services within the Security Perimeter must have unique passwords and/or access methods.
   b. Assigned administrators will be granted access only to necessary resources and no others as approved by the CA.
   c. Appropriate physical security measures should be implemented on all resources within the Security Perimeter as deemed necessary by the CA.

10. Perimeter Maintenance and Monitoring

    Key to the delivery of secure technologies is the application of routine maintenance and the performance of monitoring. This takes the form of system patches and configuration changes as advised by vendors/technical community, backups, and local/remote monitoring functions. With respect to maintenance and monitoring, the following guideline statements apply.

    a. Backups of any portion of the Security Perimeter must be performed in a secure fashion. All backup media must likewise be maintained with strict measures to ensure their security.
    b. All resources within the Security Perimeter should employ all necessary security patches and security configurations in a timely manner as determined by the CA.
    c. To the highest degree possible, all maintenance patches and configurations must be tested prior to implementation.
    d. As monitoring introduces potential security risks, local and remote, it will only be authorized in a manner approved by the CA. As security needs change, monitoring capabilities may also change.
    e. Administrators of Security Perimeter must have access to or receive notification from vulnerability advisory bodies (CERT, etc) and be responsive to applicable vulnerabilities.

11. Emergency Response

    Critical to the operation of the Security Perimeter are the methods in which administrators respond to an emergency. Contingency plans must be

available for the various emergency categories and maintained in accordance with current needs. The following plans are required for emergency response.

a. Security Breach - This includes system/resource compromise and those activities required by law enforcement to secure evidence for investigation and prosecution.
b. Virus Threat - This includes all actions necessary to mitigate and respond to virus threats.
c. System Failure - This includes system malfunction, system crash, and Internet Service provider (ISP) unavailability.

W. PRIVACY And CONFIDENTIALITY

The purpose of this guideline is to outline the steps required to safeguard or release non-public, county computer-based information.

1. Safeguarding County Information

County information must be protected from unauthorized release or disclosure. This guideline states the roles and responsibilities of all of the people involved in the creation, use, handling, storage and destruction of information.

a. Responsibilities
    1) Director of Information Systems/Chief Information Officer
        a) Provide encryption capabilities for information that is deemed highly confidential (i.e., wire transfers) as directed by the information owner.
        b) Remove information from data storage and memory of computer equipment prior to sending such equipment for maintenance, salvage, or redeployment.
        c) Protect software and data/information by including a nondisclosure agreement with outside professional services contracts.
    2) County Users/Information Systems Employees
        a) Protect information resources against unauthorized access, loss, or destruction.
        b) Keep non-public information confidential.
        c) Retain information solely for legitimate business purposes.
        d) Retrieve confidential or restricted documents immediately from fax, printers, or copy machines.
        e) Shred printed non-public data/information prior to disposal.
        f) Secure access codes and information i.e., dial-up phone number, passwords.

g) Contact the Departmental Information Security Representative or Customer Service Center staff if it is suspected that information errors are the result of illegal tampering or modification of data.

3) Departmental Information Security Representative (DISR)
   a) Investigate reports of suspected data/information tampering.
   b) Inform users about the reasons data has to be protected, legislation that affects their work, and other topics within the Information Security policies.

X. ROUTER SECURITY

This guideline applies to all routers and switches connected to County production networks, with the exception of those within DMZ areas, which fall under the *Internet DMZ guideline.* Those within internal, secured labs are excluded.

1. Router Configuration Standards

   Defined below are the minimum security configuration standards for all routers and switches connecting to a production network or used in a production capacity at or on behalf of the County.

   a. Where possible use authentication, authorization, and accounting servers to provide router access authentication and audit logging.
   b. Routers must use departmental IT-approved methods for all user authentications.
   c. The 'enable password' on the router must be kept in a secure encrypted form.
   d. Where applicable, disable the following:
      1) IP directed broadcasts.
      2) Incoming packets at the router sourced with invalid addresses.
      3) TCP small services.
      4) UDP small services.
      5) All source routing.
      6) The finger service.
      7) All web services running on router.
      8) Any protocols and services not required by the current environment.
   e. Use difficult to guess SNMP community strings if SNMP is required.
   f. Access rules are to be added as business needs arise.
   g. The router must be included in the County-wide enterprise management system with a designated point of contact.
   h. Each router must have the following statement posted in clear view: "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or

configure this device. There is no right to privacy on this device. All activities performed on this device may be logged. Unauthorized or illegal use may be a felony offense punishable under Section 502 of the California Penal Code and other laws."

i. Where possible router management must be done in one of the following ways.
   1) Locally through the console port; or
   2) Through an encrypted connection.
j. The router must be configured to take its routing updates from authorized sources only.
k. If feasible, the router will be managed via an out-of-band secure network.

Y. SEGREGATION Of DUTIES

The purpose of this guideline is to reduce the risk of having a single employee jeopardize the security of County information assets by requiring a separation of duties.

1. Separation of Duties - Work responsibilities should be segregated so that one individual does not control all critical stages of a process. Often, segregation of duties is achieved by splitting responsibilities between two or more organizational groups. Dividing duties among two or more individuals or groups diminishes the likelihood that errors and wrongful acts will go undetected because the activities of one group or individual will serve as a check on the activities of the other.

   Management should have analyzed operations and identified incompatible duties that are then segregated through policies and organizational divisions. The following functions are generally performed by different individuals: Information System's Management, systems design, application programming, systems programming, quality assurance/testing, library management/change management, computer operations, production control and scheduling, data security, data administration, and network administration.

Z. SERVER SECURITY

The purpose of this guideline is to establish the minimum standards for the base configuration of internal server equipment owned and/or operated by any County department.

1. County Owned Servers

   This guideline applies to server equipment owned and/or operated by any County department and to servers registered under any County-owned

internal network domain. Effective implementation of this guideline will minimize unauthorized access to proprietary information and technology.

2. Ownership and Responsibilities

   All internal servers deployed at the County must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by the Departmental Information Security Representative (DISR).

   Operational groups should monitor configuration compliance and implement an exception guideline tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by the DISR.

   County departments must maintain documentation on their servers. At a minimum, the following information is required.

   - Server location and primary and secondary contact(s).
   - Hardware and operating system/version.
   - Main functions and applications, if applicable.

3. General Configuration guidelines
   a. Configuration Changes - Configuration changes for production servers must follow appropriate change management procedures. Additional recommended practices follow.
      1) Operating system configuration should be in accordance with industry best practices and the County's security policies.
      2) Services and applications that will not be used must be disabled where practical.
      3) Access to services should be logged and/or protected through appropriate access-control methods.
      4) The most recent security patches must be installed on the system as soon as practical.
      5) Trust relationships between systems are a security risk and should be avoided.
      6) Use standard security principle of least privilege to perform a function. The principle of least privilege states that an object (host, service, resource, subnet, etc.) should have the minimum privileges necessary to perform its assigned task and no more.
      7) Administrators should only use their privileged account(s) when necessary and use their non-privileged account(s) in all other cases.

8) If a methodology for secure channel connection is feasible, it must be used.
9) Production servers must be physically located in an access-controlled environment.

b. System Monitoring
1) All security-related events on critical or sensitive systems must be logged and audit trails saved for a time period as determined by each County department.
2) Security-related events will be reported to the DISR, who will review logs and report incidents to management as necessary. Security-related events include but are not limited to:
- Port-scan attacks.
- Evidence of unauthorized access to privileged accounts.
- Anomalous occurrences that are not related to specific applications on the host.

c. Compliance
1) Audits will be performed on a regular basis by authorized organizations within the County.
2) The internal audit group, in accordance with the *Audit guideline*, will manage audits. Internal audit will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.

AA. SOFTWARE COPYRIGHTS And LICENSING

The purpose of this guideline is to support compliance with laws concerning software copyrights and licensing to help reduce the potential financial liability to the County.

1. Software Licensing - Use only licensed software legally acquired by the County.

2. Software Procurement - There is a significant financial liability to the County if software that has not been legally purchased is used on County-owned or leased equipment.

   Check the documentation provided with the software before you make copies for others. Generally you may make copies of software for back-up purposes only.

   It is every department's responsibility to ensure that they have valid licenses for all software used in their department.

3. Authorization of Outside Software - There is potential for introducing a virus into a County system, and possibly even Countywide, whenever outside software is used. If you need to use an outside software

program for business purposes you must first obtain permission from your department head or designee.

BB. TELECOMMUNICATIONS

The purpose of this guideline is to promote, initiate, and support secure and hardened telecommunication facilities as an information technology, mission critical strategy.

This guideline covers all telecommunications facilities transporting media for enterprise telecommunications efforts, supported by the County IT departments, including, but not limited to owned and leased facilities carrying County voice and data over fiber-optic cabling, hi-cap services, frame relay networks, Virtual Private Networks (VPN), Integrated Services Digital Network (ISDN), broad-band cable, dial-in, microwave and two-way radio facilities.

1. Telecommunications Facilities

   The Telecommunications Department installs and operates County owned telecommunications facilities. They may also form partnerships with an outside vendor to install and operate regional telecommunications facilities, in compliance with the guidelines below.

   Waivers may be granted on a case-by-case basis by the Telecommunications Department head or designee. It is the responsibility of the Telecommunications Department to maintain documentation on each waiver granted.

   a. Requirements
      1) Outside vendors and contractors shall have their employees and workers pass a security and prior criminal background check before working in the telecommunications facility.
      2) Ring down telephone shall be utilized for maintenance and technical personnel for identifying themselves upon entering the telecommunications facility to a monitoring public safety agency or Network Operations Center (NOC), 24x7x365 monitoring with a recording device.
      3) Seismic bracing shall be done to the 1997 Uniform Building Code (UBC) Seismic Zone 4 level.
      4) Smoke detection system shall be in place and monitored, with industry standard testing performed.
      5) Physical system and facility alarms (e.g. fire, intrusion, etc.) shall be monitored.
      6) Equipment failures or incidents shall be monitored on a 24/7 basis with notification going to the appropriate equipment

personnel e.g. via pager for appropriate action or as required based upon the physical attributes of the facility.

7) UPS sources should be able to notify appropriate entities of their status e.g., active, standby, offline.

b. Stand-alone Telecommunications Facilities e.g., Micro Wave Towers
   1) Outdoor or remote facilities outer perimeter fencing (recommend no less than 10 feet in height) with barbed or razor wire located at the top of the fence line.
   2) Perimeter motion detection system will monitor the facility, as deemed appropriate.
   3) Monitored closed circuit camera system that provides real-time video in infrared and visual light, covering fence line to building areas, as appropriate.
   4) Emergency backup power shall be considered in the form of two sources.
   5) Electrical power generators in place to provide a minimum of 168 hours of power to the entire telecommunications facility.
   6) Battery back-up or UPS systems able to provide a minimum of 3 hours of power if an electrical power generator is in use or 24 hours of UPS power if no electrical generator is available.

c. Telecommunication Facilities Located within Existing Structures (Buildings)
   1) Telecommunications equipment shall be located behind a secured door accessible to authorized personnel only.
   2) Entry doors shall be alarmed with monitoring devices.
   3) Battery back-up or UPS systems shall be able to provide a minimum of 3 hours of power.

CC. THIRD-PARTY I.T. SERVICE ORGANIZATION

The purpose of this guideline is to establish information security requirements for third-party Information Technology service organizations contracting with the County.

1. Requirements of Project-Sponsoring Organization - The project sponsoring organization must first establish that its project is appropriate for third-party service. The person/team wanting to use third-party service must ensure that the chosen vendor complies with this guideline.

   If the system or application is to be outsourced, a risk assessment must first be completed to determine what necessary controls must be implemented. The department must utilize the County's boiler plate contract (available through the Department of Information Technology

web site) or equivalent language to ensure protection of the County's information assets.

2. Requirements of Third Party Service Provider - The third-party service provider, if providing hosting services, must agree to provide a description of policies and controls to be utilized to protect the County's information. The third-party service provider must also have an independent audit performed at regular intervals to ensure compliance with those policies and proper implementation of controls.

   If the third-party service provider is providing support to applications or systems physically located at the County, then all access must be in compliance with existing County policies.

   The third-party service provider will ensure that any computers or systems connected to County computers, networks or systems will be patched to the most recent level and be scanned for viruses with the most recent signatures available.

DD. VIRTUAL PRIVATE NETWORK (VPN)

The purpose of this guideline is to define the minimum requirements for Virtual Private Network (VPN) connections to County networks.

1. VPN Authorization
   a. Only approved County employees and authorized third parties may use VPNs for connection to County networks.
   b. By using VPN technology with personal equipment, users understand that their machines are a de facto extension of the County's network and, as such, are subject to the same rules and regulations that apply to County-owned equipment i.e., there is no expectation of privacy.

2. User Responsibility
   a. The user is responsible for contracting with an Internet service provider (ISP).
   b. Responsibility for the installation of any required software shall be determined by the department head or his/her designee. Further details may be found in the *Remote Access Guideline*.
   c. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to the County's internal networks.

3. Configuration Requirements
   a. VPN use is to be controlled using either a one-time password authentication, such as a token device, or a public/private key system with a strong pass phrase.
   b. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel. All other traffic will be dropped.
   c. Dual (split) tunneling is not permitted; only one network connection is allowed.
   d. VPN gateways will be set up and managed by the appropriate network operational groups.
   e. VPN users will be automatically disconnected from the County's network after 30 minutes of inactivity. Pings or other artificial network processes are not to be used to keep the connection open.
   f. The VPN concentrator is limited to an absolute connection time of 24 hours.
   g. Only approved VPN clients may be used.
   h. Personnel using VPN technology with personal equipment must ensure that their machines are configured to comply with the County's security policies.

EE. WEB BROWSER CONFIGURATION

The purpose of this guideline is to define the minimum standards to ensure secure web browser configurations are used throughout the County organization. This guideline applies to all County controlled devices using web-browsers.

1. Minimum Standards
   a. Where applicable, the Home links should point to County pages.
   b. Departments shall establish the minimum security settings as deemed appropriate for their business practices.
   c. Web browser cache, history and cookies will be deleted on a regular basis in accordance with departmental guideline.
   d. Under no circumstances will web browsers be configured to store or remember passwords.

FF. WIRELESS COMMUNICATION

The purpose of this guideline is to define the minimum requirements for secure wireless communication via the County enterprise network.

This guideline covers all wireless data communication devices capable of transmitting packet data (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of the County internal networks.

1. Wireless Implementations

   Wireless implementations must conform to the following standards.
   a. Maintain point-to-point hardware encryption of at least 56 bits.
   b. Maintain a hardware address that can be registered and tracked, i.e., a MAC address.
   c. Support strong user authentication which checks against an external database such as TACACS+, RADIUS, or something similar.
   d. Must have a security guideline enforcement point (such as a firewall device) to inspect traffic prior to being allowed on the internal network.

GG. WORKSTATION CONFIGURATION

The purpose of this guideline is to define the minimum standard configurations for County workstations. This guideline applies to all workstations that connect to County networks.

1. Workstation Practices

   a. Departmental IT support staff shall ensure that the practices below are followed.
   b. Workstations will have installed only operating systems approved by the County's Department of Information Technology.
   c. All workstations configurations will comply with the County's *Patch Management, Anti-Virus,* and *Logon Banner* policies.
   d. Ability to alter operating system configuration will be limited to the level necessary to support business processes.
   e. Users will not have administrative rights to the desktop nor will they have the ability to install software.
   f. Elevated privileges will only be granted if necessary to perform work functions.

Originating department: County Administrator
Contact: Kevin Dickey, Chief Information Security Officer

_____
John Cullen
County Administrator