CONTRA COSTA COUNTY
Office of the County Administrator
ADMINISTRATIVE BULLETIN

Number: 139
Date: March 17th, 2008
Section: Information Security General Use Policy

SUBJECT: INFORMATION SECURITY – GENERAL USE POLICY

The purpose of this policy is to outline the general 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. COUNTY INFORMATION SECURITY

The purpose of this guiding principle is to define the appropriate access to, and integrity of, County information and information technology (IT) assets.

1. Minimum Standards

   The Information Security "General Use Policy" serves as the minimum standard to which all departments must adhere. Additional subordinate guidelines addressing specific areas of information security also exist. Individual departments may implement additional information security guidelines to meet their business needs but cannot establish guidelines that would supersede County guidelines.
   Information and the systems, networks, and software necessary for processing are essential County assets that must be appropriately evaluated and protected against all forms of unauthorized access, use, disclosure, modification, or denial. Security and controls for County information and associated information technology assets owned, managed, operated, maintained, or in the custody or proprietorship of the County or non-County entities must be implemented to help ensure:

   - Privacy and confidentiality
   - Authentication
   - Data integrity
   - Availability
   - Accountability
   - Audit ability
   - Appropriate use

   Department heads, board members and elected officials are responsible for ensuring information security within their department and organizational adherence to countywide guidelines and procedures. The department head will ensure the appointment of a Departmental Information Security Representative (DISR) to be responsible for managing information security within the department. This person will represent the department in the area of information security.

2. Departmental Information Security Representative (DISR)
   a. Manage information security within the department.
   b. Be responsible for any departmental information security guideline.
   c. Represent department in the County's Information Security Advisory Committee (ISAC).

d. Coordinate the Departmental Computer Incident Response Team (DCIRT).

3. Employees and Authorized Users

   Each employee and authorized user is responsible for understanding and adhering to County information security guidelines as well as appropriate organizational guidelines. They are responsible for protection of County informational assets entrusted to them and for using them for their intended purposes only. Employees will be required to sign a certificate of compliance as a condition of being granted access to County systems.

   a. Chief Information Security Officer (CISO)
      1) Chair the Countywide Information Security Advisory Committee (ISAC).
      2) Provide information security related technical, regulatory, and guideline leadership.
      3) Facilitate the implementation of County information security guidelines.
      4) Coordinate information security efforts across departmental lines.
      5) Lead continuing information security training and education efforts.
      6) Serve as an information security resource to department heads and the Board.
      7) Represent the County at professional information security forums and state and federal events related to information security.

   b. Information Security Advisory Committee (ISAC)

      The Information Security Advisory Committee will be composed of the Departmental Information Security Representatives and the CISO or designated representative. This will provide a forum for all countywide information security-related collaboration and decision-making. This is the deliberative body that will weigh the balance between heightened security and departments performing their individual business.

      1) Develop, review, and recommend information security guidelines.
      2) Develop, review, and approve best practices, standards, guidelines and procedures.
      3) Coordinate inter departmental communication and collaboration.
      4) Coordinate departmental information security education and awareness.

B. COMPUTER USE

The purpose of these guidelines is to outline the acceptable use of computer equipment at the County. These guiding principles are in place to protect the employee and the County. Inappropriate use exposes the County to risks including virus attacks, compromise of network systems and services, and legal issues.

1. General Use and Ownership
   a. Management is committed to protecting the County's employees, partners, and the organization from illegal or damaging actions by individuals by intentional or unintentional means.
   b. Internet/Intranet/Extranet-related systems, including, but not limited to, computer equipment (including PDAs), software, operating systems, storage media, network accounts providing electronic mail, Web browsing, file transfer protocol and peer-to-peer (i.e. instant messaging) are the property of the County. These systems are provided for business purposes in serving the interests of the organization and the public in the course of normal operations.
   c. While the County's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of the County. Because of the need to protect the County's network, management cannot guarantee the confidentiality of non-County, personal information stored on any network device belonging to the County.
   d. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such guidelines, employees should consult their supervisor or manager before using any county provided system for personal use.
   e. Authorized individuals within the County may monitor equipment, systems, and network traffic at any time for security, network maintenance and guideline compliance purposes.
   f. The County may conduct audits on a periodic basis to ensure compliance with this guideline.

2. Computer Security
   a. Authorized users are assigned accounts for their specific use based on their defined needs. Users are personally responsible for the security of their accounts. Passwords are provided to enable users to keep their accounts secure and should conform to the appropriate Password Guideline.
   b. Users should log off or lock the device when unattended. Password-protected screensavers with automatic activation set at 10 minutes or less is required on all PCs, laptops, and workstations. Biometrics or other authentication methods are acceptable in lieu of password protection.

c. All hosts used by the employee that are connected to the County Internet/Intranet/Extranet, whether owned by the employee or County, must continually execute approved virus scanning software with a current virus database.

d. Users must exercise extreme caution when opening e-mail attachments received from unknown senders that may contain viruses, e-mail bombs, Trojan horse code, and any other malicious code.

3. Proprietary Information

   a. Information contained on Internet/Intranet/Extranet-related systems has different sensitivity levels, such as confidential or public, as defined by the County’s regulatory and internal classification guidelines. Examples of confidential information include, but are not limited to: medical information, employee data, vendors and bidder’s sensitive information, lawyer/client correspondence, specifications, and other data. Public information is that which is maintained by an organization that is designated as “public” by law and includes a formal process for its release. Employees should take all necessary steps to prevent unauthorized access to this information.

   b. Use encryption for information that users consider sensitive or vulnerable in compliance with established standards. Users should consult their Department Information Security Representative (DISR) questions on this matter.

   c. Because information contained on portable computers, PDA’s and removable media is especially vulnerable, exercise special care in the handling, storage and transportation of this equipment.

   d. Unless posting is in the course of business duties, all postings by employees from a County e-mail address to newsgroups must contain a disclaimer stating that the opinions expressed are strictly their own and not of the County.

   e. Providing confidential information about, or lists of, County employees to parties outside the County is strictly prohibited.

4. Unacceptable Use

   Illegal activities under local, state, federal, or international laws are strictly prohibited. The lists below are by no means exhaustive but attempt to provide a framework for activities that fall into the category of unacceptable use. Examples of prohibited activities include:

   a. System and Network Activities

      1) Utilization of products that are not appropriately licensed and approved for use by the County or those that violate the rights of any person or organization protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations,

including, but not limited to, the installation or distribution of "pirated" or other software.

2) Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the County or the end user does not have an active license.
3) Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws is illegal. Consult the appropriate management prior to exporting any material that is in question.
4) Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5) Using a County computing asset to actively engage in procuring or transmitting material in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
6) Making fraudulent offers of products, items, or services originating from any County account.
7) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
8) The introduction of any software or hardware onto any County system or network without prior written consent from the Departmental Information Security Representative (DISR). If the desired connection will have access to the Wide Area Network (WAN), then additional authorization must come from the Department of Information Technology (DoIT) WAN support staff.
9) Port scanning or security scanning unless these are within defined job duties and specifically authorized by management.
10) Executing any form of network monitoring that will intercept data not intended for the employee's host, unless these are within defined job duties and specifically authorized by management.
11) Circumventing user authentication or security of any host, network, or account.
12) Interfering with or denying service to any user (e.g., denial of service attack).
13) Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

b. E-mail and Communications Activities
   1) Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (i.e. e-mail spam).
   2) Any form of harassment via e-mail, telephone or paging, whether through language, frequency, or size of messages.
   3) Unauthorized use or forging of e-mail header information.
   4) Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.
   5) Creating or forwarding "chain letters," "Ponzi," or other "pyramid" schemes of any type.
   6) Use of non-County email to conduct County business.1
   7) Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

C. <u>SECURITY AWARENESS TRAINING & EDUCATION (SATE)</u>

This guiding principle sets forth the minimum standard for Security Awareness Training & Education (SATE) to reduce the County's informational security risk. Each department is responsible for ensuring that all employees are trained to at least this minimum standard. In certain situations it will be necessary for departments to provide additional training.

1. SATE is crucial to minimizing the County's exposure to both malicious threats and accidental errors and omissions. SATE is not only defined by industry best practices, it is also to ensure that employees are aware that there are legal statues that cover the protection of the information owned by the County (for example, CA Penal Code 502, HIPAA, Computer Security Act of 1987).

2. A secondary purpose of SATE is to document employees' knowledge and understanding of guidelines and procedures, allowing for disciplinary action when required and development of good working habits.

3. Questions about SATE should be addressed to one's manager.

4. The term "Security Awareness" is considered the daily "moment-by-moment" awareness level while the term "Security Training" relates to the basic training all employees need to build their basic security skills. Security Awareness is partially a by-product of training, but it also is the result of environmental factors.

5. Most County employees will only need the minimum level of security training as follows.
   a. Incorporate basic security training for all new hires, ideally before a new hire sits down to do his or her job.

b. Include in the training curriculum “social engineering” techniques that hackers use to gather information.
c. All employees must attend security guideline training classes and be tested for basic security awareness at least every two years.
d. Explain to employees that while their departments are the “owners” of the data, they need to assist the Information Systems department in its safekeeping.
e. Explain to employees the difference between “public” records and the need to keep information “confidential.”
f. State reasons why specific guidelines are needed.
g. Describe what is covered by the guidelines.
h. Define guideline contacts.
i. Define user’s responsibilities.
j. Define how violations will be handled.

6. Certain employees may require more frequent and in-depth training due to their high level of access to information.

7. While security training is a clear concept, the concept of security awareness is a bit more ambiguous. It deals with the level of security consciousness. Therefore, we are talking about various “reminders” or “visual cues” that can be used to help users “think security”.

8. Following are some basic elements needed to increase security awareness.
   a. Pre-Login “Splash Screen” with usage warning. Must point to the county’s Acceptable Usage documentation.
   b. Posters and e-mails.
   c. Web sites.
   d. Periodic meetings, contests, and positive reinforcement.
   e. Printable Security Newsletter available from Intranet security web site.

D. <u>LOGON BANNER</u>

The purpose of this guideline is to define and set the minimum standards for applying a logon banner that will inform users of their responsibilities when accessing County network and computer systems.

All Information Systems capable of displaying system messages must display, as the first message seen by the user, a warning that the system being accessed is a County Information System and is for official use only.

1. Accessing County Information Systems

   To establish a reasonable expectation that employees have been notified of the existence of acceptable usage expectations, to limit the expectation of user privacy, and to be able to prosecute violators, (especially under Public Laws 98-473 and 99-474) the County has established a Logon Banner that notifies employees of these limitations.

The Logon Banner includes incorporates recommendations from the Department of Justice on what should be included in such a warning.

a. The word “WELCOME” should not appear in the first logon screen. This could imply that anyone is welcome to access and use the system.

   Understand, this does not mean that every screen accessing each application needs this warning, only the first screen seen by anyone accessing a County platform (e.g., standalone PC, Network).

> “This system is for authorized use only. All activities may be recorded and monitored. There are no implicit or explicit rights to privacy using this system. Unauthorized or illegal use may be a felony offense punishable under Section 502 of the California Penal Code and/or other laws.
>
> *Pressing any key will continue and by doing so, you accept these terms!*
> *or*
> *Your use of this system indicates your acceptance of these terms!”*

2. Employees must be advised that they are subject to having their activities monitored and that use of the system implies consent to such monitoring.

3. Employees need to know that information gathered may be given to law enforcement or other investigative officials for action if warranted.

4. Employees must be aware of the impact of inappropriate use/access.

5. Employees must acknowledge this warning by some positive action on their part, like a keystroke.

6. Monitoring

   Employees must be aware that their actions might be monitored. The following is an example of monitoring verbiage.

> "All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Such information includes sensitive data encrypted to comply with confidentiality and privacy requirements. Access or use of this computer system by any person, whether authorized or unauthorized, constitutes consent to these terms. There is no right of privacy in this system."

E. <u>E-MAIL</u>

This purpose of this guideline is to define the use of County e-mail communications. E-mail communications are to be used in a professional manner and only for County purposes.

1. Procedures for Use
   a. Each County Department must define procedures for incidental and non-business use of County information technology resources.
   b. Access to e-mail services is a privilege that may be wholly or partially restricted without prior notice or without consent of the user.
   c. All e-mail messages are the property of the County and subject to review by authorized County personnel.
      - Staff cannot expect a right to privacy when using the County e-mail system.
   d. All e-mail is subject to audit and periodic unannounced review by authorized individuals as directed by the Director of each Department.
   e. The County reserves the right to override any individual password and access all electronic mail messages for any business purpose. Therefore, all employees must recognize that incoming and outgoing messages are not private.
   f. E-mail is subject to the guidelines concerning other forms of communication as well as all other applicable guidelines including, but not limited to, confidentiality, conflict of interest, general conduct and sexual harassment.
   g. E-mail services shall not be used for purposes that could reasonably be expected to cause directly or indirectly excessive strain on the e-mail system or unwarranted or unsolicited interference with others' use of e-mail or the e-mail system.
   h. E-mail communications must be secure to:
      - Prevent unauthorized access.

- Prevent unintended loss or malicious destruction of data and to provide for the integrity and availability of all e-mail systems.

i. County Departments shall take appropriate steps to protect all e-mail servers from various types of security threats as follows:
   1) Place e-mail servers in safe locations that are physically secured. See the "Physical Security" guideline for more information.
   2) Back-up e-mail servers for software and data on a regular basis. See the "Business Continuity" guideline for more information.
   3) Maintain current anti-virus software on e-mail servers.
   4) All County Departments must have appropriate procedures in place to monitor personnel having administrative access to e-mail servers.

j. County departments shall develop guidelines regarding the use of e-mail services not provided by the County. Such guidelines shall ensure the integrity of the County e-mail process. County departments and e-mail users must understand that a County-owned asset cannot reside on non-County-owned resources where the County has no jurisdiction.

k. County departments shall determine an e-mail data retention guideline as applicable to their security requirements. Retention of e-mail should be kept to the minimum required by law and business purposes.

l. Encryption of e-mail may be appropriate in some instances to secure the contents of an e-mail message. Each user should be cognizant of the sensitivity of information contained in e-mail and understand that it may be passed beyond the intended recipient. Encryption must follow County standards.

m. E-mail systems must provide for authentication of the user for all remote e-mail users.

F. PASSWORD

This purpose of this guideline is to establish a standard for reference when: creating strong passwords; the protection of those passwords; and the frequency of change.

1. Password Protection

Passwords are an important aspect of computer security and are usually the front line of protection for user accounts. A poorly chosen password may result in the compromise of the County's entire enterprise network. As such, all County employees (including contractors, vendors, and temporary staff with access to County systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Password Guidelines
   a. All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed at least every 30 days.
   b. All production system-level passwords must be part of the security administered global password management database.
   c. All user-level passwords (e.g., e-mail, applications, Web, desktop computer, etc.) must be changed at least every 90 days. The recommended change interval is every 60 days.
   d. User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
   e. Passwords must not be inserted into e-mail messages or other forms of electronic communication.
   f. Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of “public,” “private,” and “system,” and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
   g. All user-level and system-level passwords must conform to the guidelines described below.

3. Poor or Weak Password Characteristics
   a. The password contains less than eight characters.
   b. The password is a word found in a dictionary (English or foreign).
   c. The password is a common usage word, e.g., names of family, pets, friends, coworkers, fantasy characters, etc.
   d. Computer terms and names, commands, sites, companies, hardware, software.
   e. The word Contra Costa or any derivation.
   f. Birthdays and other personal information such as addresses and phone numbers.
   g. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
   h. Any of the above spelled backwards.
   i. Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

4. Strong Password Characteristics
   a. The password is at least eight alphanumeric characters in length and contains both upper and lower case characters along with special characters. Examples include:
      - a-z
      - A-Z
      - 0-9
      - Special Characters: ! @ # $ % ^ & * ( ) + ~ - = \ ‘ { } [ ] : ; “ ‘ < > ? , . /
      - Not all systems allow for the use of these characters.

b. Select a password that is not a single word in any language, slang, dialect, jargon, etc.
c. Avoid creating a password based on personal information e.g., names of family, etc.
d. Passwords should never be written down (unless stored in a locked safe for recovery purposes) or stored online. Instead, try to create passwords that can be easily remembered yet hard to guess.

   Example: Create a password based on a song title, affirmation, or other phrase. The phrase might be: “This May Be One Way To Remember” and the password could be: “TmB1w2R!” or “Tmb1W>r~” or some other variation.

   Note: Do not use either of these examples as passwords!

5. Password Protection Standards
   a. A password is changed at least once every 90 days. The exception is a system-level password that must be changed every 30 days.
   b. Do not use the same password for County accounts as for other non-County access e.g., personal Internet Service Provider (ISP) account, option trading, benefits, etc.
   c. Avoid using the same password for various County access needs. Instead, select one password for the network systems and a separate password for application systems.
   d. Select a separate password to be used for a NT account and an AS400 or UNIX account.
   e. Do not share County passwords with anyone e.g., administrative assistants, secretaries, etc.
   f. Treat all passwords as sensitive and confidential County information.
   g. Avoid giving your password over the phone to ANYONE.
   h. Do not send a password in an e-mail message.
   i. Avoid talking about a password in front of others.
   j. Do not hint at the format of a password e.g., “my family name.”
   k. Never write your password on questionnaires or security forms.
   l. Do not share your password with others.
   m. If someone demands a password, refer him or her to this document or have him or her call someone in Information Security.
   n. Never use the “Remember Password” feature of applications e.g., Eudora, Outlook, Netscape Messenger.
   o. If you must write your passwords down, store them in a secure place and never anywhere in your office.
   p. Passwords stored in a file on ANY computer system e.g., Palm Pilots or similar devices, can be compromised if encryption isn’t used to secure them.

q. If you suspect that your account or password is compromised, report the incident per the Incident Response Guideline and change all passwords.
r. Password strength checking may be performed on a periodic or random basis by departmental or county IT or its delegates. Any weak passwords found during one of these scans may require the user to change it.

6. Application Development Standards

   Application Developers must:
   a. Ensure that their applications support authentication of individual users, and not groups.
   b. Not store passwords in clear text or in any easily reversible form.
   c. Provide for some sort of role management, so that one user can take over the functions of another without having to know the other's password.
   d. Ensure that their application(s) support Terminal Access Controller Access Control System (TACACS+), Remote Authentication Dial-In User Service (RADIUS), and/or X.509 with Lightweight Directory Access Protocol (LDAP) security retrieval.

7. Use of Passwords and Passphrases for Remote Access Users
   a. All of the above guidelines that apply to passwords also apply to passphrases.
   b. Access to the County networks via remote access is to be controlled using either a one-time password authentication (e.g., token) or public/private key system with a strong pass phrase.
   c. A passphrase is composed of multiple words providing greater security against password "dictionary attacks."
   d. A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase: "IwishIwasinHawaii!"

G. VIRUS PROTECTION

The purpose of this guideline is to ensure that all County electronic data devices are protected by installed and actively maintained anti-virus software. This includes:

- Personal Computers e.g., desktops, laptops, hand-held devices
- Servers

1. Viruses

   A virus is a piece of self-replicating code, most often a malicious software program designed to destroy or damage information on computers. Some viruses cause no damage, but a significant number are specifically designed to cause data loss. Potential sources of viruses include shared media such as floppy disks or CDs, e-mail, and content downloaded from the Internet.

   A virus infection is almost always costly to the County whether through the loss of data; staff time to recover a system, or the delay of important work.

   Computer viruses may impact the entire County and not just a specific department as all County departments share countywide systems e.g., e-mail system, shared network infrastructure.

   In a networked environment, the weakest link in the chain can breach the security of the information on the entire network.

   a. Role of Information Technology
      1) Define enterprise anti-virus solutions and negotiate volume purchases for the County as a whole.
      2) Architect and monitor the overall design, function, and effectiveness of the anti-virus protection systems throughout the County.
      3) Inform departments of recommended operating system and application patches that are required to protect against potential system security problems.
      4) Provide guidelines on installing and maintaining anti-virus software and pattern file updates on departmental servers and workstations.
      5) Set up servers that will regularly check for new virus pattern files and update them as needed. Departmental servers will download the new pattern files from these servers.
      6) Proactively notify departmental IT contacts of high-risk viruses as soon as they are known to be in circulation. Appropriate staff (e.g., WAN, IT Security, Customer Services) will distribute information or warnings regarding viruses to departmental IT staff or end users, when appropriate, and serve as a clearing house to communicate virus incident information received from departments or outside sources.
   b. Role of Department
      1) Ensure that all departmental servers and workstations have current anti-virus software installed.
      2) Ensure that once installed, anti-virus software is not disabled on servers or workstations.
      3) Perform day-to-day administration of their anti-virus servers.

4) Apply any recommended operating system and application patches to protect against potential system security problems.
5) Notification of any virus or network security-related incidents.
6) Designate a primary and an alternate coordinator who can be contacted and is able to participate in the event of a significant virus incident.

c. Role of Individual User

1) Exercise caution when opening email attachments. Users should not open attachments that they do not expect or from users they do not know.
2) Exercise extreme caution when downloading files from the Internet. Files should only be downloaded from reputable sites.
3) Report virus incidents to their departmental IT staff and, if known, provide them with the following information:
   - The name of the parties involved e.g., e-mail received from, or infected file on a server, etc.
   - Virus name or type.
   - The source of virus e.g., e-mail, Internet download, floppy diskette, etc.
4) Once anti-virus software is installed on a workstation, users are not to modify the software or its configuration in any manner, unless directed by IT departmental personnel.
5) Follow the appropriate guidelines and keep personal use of County equipment to a minimum to reduce the possibility of receiving virus-infected e-mail on County equipment.

H. PHYSICAL SECURITY

The purpose of this guideline is to describe the responsibilities for protecting physical computers and information resources, including non-computer informational assets.

1. Protection of Informational Assets

The County requires that appropriate environmental, protective, and access control systems are in place to protect physical computers and information resources including non-computer informational assets. Proper and adequate physical security and protection of hardware, software, and other County-controlled assets are the responsibility of all County employees.

2. Responsibilities

a. All Employees

1) Secure information resources and equipment at all times.

2) When applicable, report the loss or theft of any information resource to management immediately and complete required forms.
3) Request identity for any person(s) or activities unknown to you or that appear not to belong at a given physical location.
4) Ensure proper disposal of information assets based upon departmental, local, state, or federal law or guideline.

b. Information Systems Employees

- Inventory and store data file backup information at an off-site location as per established retention schedules.

c. Director/CIO of Information Systems

1) Identify and enforce physical security requirements.
2) Identify requirements for environmental protection of the computer center and any remote facilities.
3) Limit distribution of computer center access codes or keys e.g., hard, proximity, magnetic stripe, and combinations only to those employees needing entry to fulfill their job requirements.
4) Develop and keep current an inventory of physical computer and information resources including peripherals.
5) Develop and keep current a list of authorized service vendors entering the computer center for repair and maintenance of equipment.
6) Authorize a County escort for any person whose access to the computer center is not a job requirement.

d. Security Administrator

1) Review and retain logs for system level security violations and retain records per the established retention schedule.
2) Oversee physical security requirements for the computer center facilities.
3) Maintain records of individuals assigned access codes/keys/combinations.

e. Internal Auditor

1) Audit the computer center to determine compliance with the above guideline.
2) Review physical security considerations and recommend appropriate controls.
3) Evaluate the effectiveness of environmental controls.

I. CLEAR DESK

The purpose of this guideline is to define the minimum standards necessary to reduce the risk of unauthorized access, loss of, or damage to County information assets contained in employee work spaces. It also recommends the minimum requirements for securing County information assets.

1. Where appropriate, store paper documents and computer media with sensitive information in suitable containers when not in use, even during working hours.

2. Lock away classified material when not needed, especially when the office is unoccupied.

3. Do not leave sensitive information on white boards, peg boards, bulletin boards and other visible media.

4. Log off personal computers and computer terminals when unattended.

5. Protect personal computers and computer terminals by key locks, passwords or other controls when not in use.

6. Protect incoming and outgoing mail points and unattended fax and telex machines.

7. Lock photocopiers outside of normal working hours (or protect from unauthorized use in some other way)

8. Clear classified information from printers and photocopiers immediately.

J. REMOTE ACCESS

The purpose of this guideline is to ensure that only authorized access is allowed to the County's computer network from a location that is not physically connected to the County network i.e., a remote site.

This guideline applies to all computer and data communications systems administered by the County or for the County by authorized IT service providers.

1. Granting Remote Access
   a. Remote access is granted for authorized County work.
   b. All remote access to the County WAN will be accomplished via a secure remote access method i.e., strong authentication, Virtual Private Network (VPN), controlled dial-in/dial-out, firewall demilitarized zone (DMZ)).
   c. Internet services will be strictly controlled by firewall technology to provide preventative and detective controls.
   d. Access from a remote site to a County network that contains SENSITIVE or RESTRICTED information, as defined in the Information Classification guideline, requires extended identification and authentication procedures.

e. All employees accessing the County network from their privately-owned computers will exercise due diligence in ensuring that their systems (both hardware and software) are free from computer viral infection and unauthorized use.

f. When an authorized user terminates County employment or transfers to another County department, office or agency, all existing remote access services will be terminated.

g. Remote access will have to be re-justified and re-established for any new County position. County-owned hardware must be returned to the County and software permanently deleted from privately owned equipment.

2. Responsibilities

   a. Information Technology

      1) Provide liaison with other departments regarding remote access usage.
      2) Manage the infrastructure for remote access for County-authorized users.
      3) Determine the risk of remote access and implement acceptable, approved solutions to manage the risk

   b. Departmental

      1) Ensure that all County and departmental remote access guidelines are implemented and reviewed for compliance.
      2) Manage and approve end-user business case requests for remote access and resources.
      3) Manage the infrastructure for remote access and use when the department is providing this service for their customers.

   c. End User

      1) Follow County and departmental practices and guidelines as they relate to remote access.
      2) Follow County and departmental guidelines regarding information disclosure.

K. <u>PORTABLE COMPUTING AND MEDIA</u>

The purpose of this guideline is to define the minimum requirements for securing all portable computing and media devices. Examples include: Personal Digital Assistants (PDA), USB drives, laptops, etc.

Due to the prevalence of portable media used in enhancing productivity and convenience, organizational controls and oversight are paramount. This guideline is designed to ensure that the mobility and ease of use does not lead to inadvertent or accidental disclosure, loss or misuse of County informational assets.

1. Controls for Portable Computing and Media Devices

   Portable Computing and Media controls shall include the following items:

   - County informational assets should only be copied onto portable media when there is a valid business practice.
   - Any informational asset stored on portable media shall be secured as specified in the *Information Classification Guideline.*

2. Education of employees in the proper use of portable media.

   Depending on the type of device, file protection tools should be enabled to protect any information stored on portable media. This may include, but is not limited to encryption, passwords, third party products, encrypted file systems or other security measures.

   - Portable media should be securely stored and safeguarded at all times.
   - Portable media used to backup informational assets shall adhere to the *Backup and Recovery Guideline.*

3. Portable Media Disposal

   Disposal of portable media should be sanitized in accordance with Administrative Bulletin 517 and the *Mass Storage Decommissioning Guideline.*

L. <u>INCIDENT RESPONSE</u>

The purpose of this guideline is to outline the required steps to be taken in the event of a real, perceived or potential security incident. Due to a variety of issues, it is imperative that a formal reporting and response guideline be followed when responding to security incidents.

1. Department Responsibility

   Notify the Departmental Information Security Representative (DISR) immediately of any suspected or real security incident. If the DISR is not available, the user must notify their immediate supervisor. If it is unclear as to whether a situation should be considered a security incident, the DISR should be contacted to evaluate the situation.

   Only qualified personnel are to take action on any investigation or corrective action situation.

2. Individual User Responsibility
   - Report any perceived security incidents to the DISR.

3. DISR Responsibility
   a. Evaluate the security incident situation.
   b. Take initial action to isolate and contain the situation.
   c. Keep a record of actions taken.
   d. Contact the Computer Incident Response Team (CIRT) if further assistance is required.
   e. Submit a Security Incident Report.

4. CIRT
   a. Respond to security incidents as required.
   b. Coordinate with Law Enforcement Agencies or the Hi-Tech Crimes Unit, as required.

5. Chief Information Security Officer (CISO)
   a. Review Security Incident Reports.
   b. Compile and maintain security incident statistics County Administrator.

M. <u>BUSINESS CONTINUITY</u>

The purpose of this guideline is to define the County's Business Continuity Planning (BCP) efforts and functions, and assigns roles and responsibilities for this effort.

1. Business Impact Analysis (BIA)
   - The BIA identifies what processes and resources are needed by the business unit for a specified disaster scenario. The duration of a disaster can be either short or long term.

2. Information Technology (IT) Backup and Recovery Plan (aka Operational Recovery Plan)
   - The Operational Recovery Plan defines how to recover mission critical technology and applications at an alternative site as required by the County statute governing the business unit. The plan includes: IT data backups, storage, and data restoration procedures.

3. Business Contingency, Recovery and Restoration Plan

   This plan defines how to continue business without "normal" resources, recover mission-critical processes at alternative sites, and restore normal business functions at permanent facilities. Current copies of a department's business continuity plans will also be stored offsite at an alternate location for use during an emergency situation.

Testing of the plan will be conducted at least annually with periodic review of the plan. As part of change control, any system, application, or network change must be reflected or considered in the BCP.

Updates and revisions to the BCP will be distributed to all employees involved in the recovery process, including Risk Management and the County's Office of Emergency Services (OES), as applicable. This guideline is in conjunction with AB115 (hyperlink)

N. <u>RISK ASSESSMENT</u>

This guideline Identifies and authorizes individuals charged with responsibility of assessing risk, the security guidelines and procedures to be enforced in order to initiate appropriate remediation and requires the performance of periodic information security risk assessments for the purpose of determining areas of vulnerability.

1. Risk Assessment Performance

   The performance of Risk Assessment is a critical business function that identifies and secures vulnerabilities within an information system's environment. Therefore, the performance of this guideline requires the full cooperation of those involved with any Risk Assessment, be they directly or indirectly involved with the area being assessed.

   The execution, development and implementation of vulnerability remediation likewise require full cooperation. It is the joint responsibility of the Risk Assessment Authority and those responsible for the area being assessed to perform effective remediation.

2. The Chief Information Security Officer (CISO) or CISO's designee(s)

   The CISO is responsible for the appointment of Risk Assessment Authorities.

   Under the direction of the CISO or CISO's designee(s) the Risk Assessment Authorities have the authority to periodically conduct risk assessments to ensure the acceptable operation of the area assessed.

3. Conducting Risk Assessments
   a. Under the jurisdiction, authority, and responsibility of the Information Security Program's Chief Information Security Officer (CISO), Risk Assessments can be conducted on any entity within the County governance structure. This includes but is not limited to any information system, application, server, network, facility, and/or any

process/procedure by which these systems or facilities are administered and/or maintained.

b. All Risk Assessment findings will be documented and confidential to the necessary parties identified at Risk Assessment commencement.
c. The activities of Risk Assessment Authorities will not be compromised.
d. Risk Assessments will be conducted with the proper security clearances and will be conducted with the full cooperation of those responsible for the area assessed.

4. Vulnerabilities
   a. Identified vulnerabilities will be assessed for criticality.
   b. All vulnerabilities that unnecessarily endanger or expose resources must be immediately remediated.
   c. All vulnerabilities identified for remediation must be reported to and acknowledged by the CISO or the CISO's designees.

O. DATA CENTER OPERATIONS

The purpose of this document is to define the minimum standards for hosting computing assets, and their respective conditions of use. This guideline applies to the data center managed and operated by the County's Department of Information Technology (DoIT). Departmental data centers shall adhere to the same requirements where applicable.

1. Services

   The County Data Center provides computing assets for a variety of enterprise-based computing solutions. These solutions are primarily, but not limited to, that which supports the enterprise computing model. In addition, the Data Center hosts departmentally maintained solutions, and those acquired with commercial off the shelf (COTS) applications.

2. Use of Computing Assets
   a. County staff, customers, and vendors shall use the computing assets in a manner consistent with County guidelines.
   b. Users shall not use County computing assets to solicit or transact personal business for gain of any kind. All activities shall be limited to the furtherance of the County's business function(s).
   c. Users shall respect the privacy of others. They shall not obtain passwords or gain access to the accounts or machines of other users by any means.
   d. Users shall not intentionally seek information about, obtain copies of, or modify files, tapes or any data belonging to other users, unless they have been given explicit authorization to do so by those users, and then only for the purposes intended by the County.

e. Users shall not attempt to infiltrate or gain unauthorized access of any kind to the Data Center, damage the computing assets, nor alter the components of the computing assets.
f. Users shall not accept or give unauthorized access to the Data Center. Access codes and user IDs are for the exclusive use of the individuals to whom assigned.
g. Data Center documentation should not be removed unless prior authorization is obtained from the Data Center Manager.

3. Responsible Use

The Data Center will be used in a responsible and efficient manner, consistent with the goals of the County. Users are expected to:

a. Honor any current computer system resource usage guidelines.
b. Refrain from engaging in wasteful practices such as unnecessary printer listings, holding of computer system resources, such as workstation consoles, and excessive use of the network.
c. Keep all operational areas clean.
d. Honor all guidelines specifying the priority of production work.
e. Maintain current software patches and anti-virus updates for/on any computer within the Data Center.

4. Hardware Additions, Deletions, and Changes

a. Requesting changes in Data Center hardware is done via the DoIT's Help Desk, submitted to the Data Center Operations supervisor.
b. Upon receipt of the change request, Data Center staff will ensure the following assessments are performed:
a. Electrical power
b. UPS capacity
c. Generator capacity
d. Adequate floor or rack space
e. HVAC
f. Backup/archive procedures
g. Network capacity
h. Establishing appropriate hardware and software maintenance contracts.

NOTE: Allow 2-4 weeks for a complete reply from the Data Center Operations Supervisor.

5. Tape Library

a. Part/parcel to hosting computing solutions, is the presence of a universal tape library.
b. The tape library system shall consist of multiple vaulting locations:
   - Within the Data Center.

- A secondary location within driving distance; and
- A tertiary site at a greater distance, outside the same geographical threats for disaster recovery.

c. Tape rotation through the Data Center's vaulting locations, the number of tape media stored, and the generational schema will be established with the Data Center Operations supervisor at such time as the computing solution is placed into a production status.
d. The Information Owner must provide a written statement to the Data Center Operations supervisor if no backup/archive is required.

6. File Restoration
   a. File restoration is a normal service of the Data Center.
   b. Files are restored from the system backups, with procedures supplied to the Data Center, by the Information Owner, at the time the computing solution is moved into production.
   c. File restorations are performed on a first-come, first-served basis, and are generally performed as quickly as possible for the user.
   d. The official guideline is that the file will be restored within 24-48 hours of the time it is requested, unless otherwise agreed upon.

7. Printing, Computer Output Microfiche, CD-ROM

   All output generated from the Data Center shall be distributed directly to known representatives of the departments/agencies they serve per process documentation.

8. System Maintenance
   a. Routine software/hardware maintenance shall be scheduled and prior notification shall be posted two (2) working days in advance.
   b. Emergency outages during normal business hours are out of the control of the Data Center staff and notification will be sent ASAP.

9. Computer Operations Center Tours

   School classes, clubs and visitors may arrange in advance to take a short, guided tour of the Data Center subject to the approval of the Data Center Operations supervisor.

P. PROJECT DEVELOPMENT LIFE CYCLE (DLC)

The purpose of this guideline is to *proactively* ensure that Applications, Systems and Services are properly designed and maintained to meet County budgetary requirements, security guidelines and end-user functionality and fulfill the business objectives. This is accomplished by implementing a formal Project Developmental Life Cycle (DLC) process.

1. DLC Process

   The DLC is a phased approach during which defined work products and documents are created, reviewed, refined, and approved. The final phase occurs when the system is disposed of, and the business need is either eliminated or transferred to other systems.

   Not every project will require that the phases be subsequently executed. The DLC may be tailored within a department to accommodate the unique aspects of a project as long as the resulting approach remains consistent with the primary objective to deliver a quality system.

   DLC phases may overlap and projects can follow an evolutionary development strategy that provides for incremental delivery of products and/or subsystems. A formal DLC ensures the following:

   a. Delivery of quality applications, systems, and services that meet or exceed customer expectations on time and within cost.
   b. A framework for developing quality and secure applications, systems, and services using an identifiable, measurable, and repeatable process.
   c. A project management structure to ensure that each development project is effectively managed throughout its life cycle.
   d. Identification and assignment of roles and responsibilities for all stakeholders including functional and technical managers.
   e. Project development requirements are well defined and objectives met.

2. Project Process Groups

   Each process group has associated critical success factors that must be achieved to ensure a successful project. Examples include:

   a. Project Scope Management
   b. Project Documentation
   c. Stakeholder Communication
   d. Regular Review of Expenditures
   e. Risk Identification and Mitigation
   f. Staffing and Required Skills as they relate to Deliverables
   g. Support

   It is important that key stakeholders, including customers and security be involved to ensure project success.

3. Project Life Cycle

   The five primary process groups of the project developmental life cycle are:

   a. Initiate – Defines and authorizes the project.
   b. Plan – Defines and refines objectives, and plans the course of action required to attain the objectives and scope that the project was undertaken to address.
   c. Execute – Integrates people and other resources to carry out the project management plan for the project.
   d. Monitor/Control – Regularly measures and monitors progress to identify variances from the project management plan so that corrective action and be taken when necessary to meet project objectives.
   e. Close – Formalizes acceptance of the deliverable e.g., product, service or result and brings the project to an orderly end.

4. Project Deliverables

   Project deliverables will be accomplished by the following:

   a. Establishing appropriate levels of management authority to provide timely direction, coordination, control, review, and approval of the development project.
   b. Ensuring project management accountability.
   c. Documenting all requirements (e.g., functions, laws, guidelines) and maintaining trace ability of those requirements throughout the development and implementation process.
   d. Ensuring that projects are developed within the current and planned information technology infrastructure.
   e. Identifying and mitigating project risks.
   f. Coordinating and ensuring that the required support is provided.

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

John Cullen
County Administrator