California County Information Services Directors Association

California Counties "Best Policies" for the Countywide Information Security Program

CCISDA Information Security Forum
April 2003

Contributing Authors to County Information Security Program "Best Policies"

County of Alameda	Leslie Simmons, Supervisor - Production Support Unit
County of Contra Costa	Kevin Dickey, Chief Information Security Officer
County of Fresno	Wincy Carr, Division Manager
County of Kern	Jefferson Huot, (Policy Task Force Co-Chair), Network Systems Administrator
County of Los Angeles	Al Brusewitz, Chief Information Security Officer Robert Pittman, Assistant Chief Information Security Officer
County of Orange	Jack Miller, CISSP, Chief Information Security Officer
County of Sacramento	Chas Lesley, Enterprise Security Adam C. Huyck, CISSP, Enterprise Security
County of Shasta	David Cutler, Computer Systems Specialist
County of Ventura	Robert Wood (Policy Task Force Co-Chair), Information Security Officer

Special Thanks to CCISDA Information Security Forum Members from

County of Calaveras

County of Colusa

County of El Dorado

County of Kern

County of Kings

County of Lake

County of Madera

County of Marin

County of Mendocino

County of Monterey

County of Napa

County of Nevada

County of Placer

County of Riverside

County of San Bernardino

County of San Joaquin

County of Santa Barbara

County of Santa Clara

County of Shasta

County of Solano

County of Stanislaus

County of Sutter

County of Tuolumne

County of Yolo

Special Thanks to: Dave Lyons, Vanguard Integrity Professionals
Dean Hipwell, CISSP, of Dean Hipwell and Associates

Table of Contents

Executive Summary

Introduction

In March 2002, the CCISDA Information Security Forum (ISF) released its ‘Information Security Program - Best Practices’ that has been adopted by many counties since that time. As a logical follow-up, the ISF established another task-group to draft Information Security ‘Best Policies’, a natural progression of the ‘Best Practices Program’. These policies are intended to be adopted by the Board of Supervisors in each County, and are drafted to target the Countywide policy directives in each County. That is to say that these are Board level policies, and meant to be used at the County level throughout each individual County Department.

What are Information Security Policies and Why Have Them?

The security-related decisions we make, as County employees and executives, largely determine how secure or insecure our information assets are, how much functionality our computerized resources offer, and how informational assets are maintained throughout the County.

Every organization (private or public) has policies that direct employees and customers on what can and should be expected from the organization. County government is no exception. Policies allow people to understand what is expected of them, and what they are accountable for. Information security policies allow organizations to be able to perform certain functions in a cost effective and cost efficient manner.

Most information security policies are based upon law or moral and ethical conducts. They must be implemented and enforceable, concise and easy to understand, and balance protection with productivity. The policies within this document do the same. They are drafted using industry proven standards and are to allow county governments the ability to comply with the various laws (Federal, State, and Local) as well as ensure that taxpayer’s assets are being used according to the laws and local jurisdictions.

Expect the Unexpected

Imagine what might happen if…

Essential data were stolen, lost, compromised, corrupted, or deleted?

Email systems were down for a day or more? What would the cost of lost productivity be?

Citizens were unable to get County supplied services?

Preparing for multiple business disruptive scenarios seems to be a growing trend, especially in light of the World Trade Center and Pentagon attacks on September 11, 2001, and potential conflicts around the world involving the United Nations and the USA. Government needs to prepare for disruption of services and in protecting those informational resources under their direct charge. In a report released by the Giga Information Group concerning trends expected in 2002, they stated that corporate executives would be increasingly willing to take a direct interest in security preparedness against physical disasters, cyber-terrorism and espionage. We must and will meet that challenge as well.

Having a comprehensive information security program and supportable policies in place provides intrinsic value for the County. It will also enhance the credibility and reputation of each County that adopts them and increase confidence from employees and citizens alike.

Best Policies of an Information Security Program, an Executive Perspective

Purposes of Information Security Policies

The main purpose of an information security policy is to inform users, staff and managers of their obligatory requirements for protecting technology and information assets. The policies should specify the mechanisms through which these requirements can be met. Another purpose is to provide a baseline from which to acquire, configure and audit computer systems and networks for compliance with the policy. Therefore, an attempt to use a set of security tools in the absence of at least an implied security policy is futile.

Who should be Involved When Forming Policy?

In order for an information security policy to be appropriate and effective, it needs to have the acceptance and support of all levels of employees within the organization. It is especially important that county management and appointed and elected officials fully support the information security policy process otherwise there is little chance that they will have the intended impact. The following is a list of individuals who should be involved in the creation and/or review and approval of information security policy documents:

Chief Information Security Officer

Information technology staff (e.g., staff from computer support units)

Department Heads and Elected Officials and administrators of groups within the organization (e.g., business departments)

Information Security Advisory Committee

Executive Management

Other responsible management

Legal Counsel

Internal IT audit

Human Resources

Employee Unions (for notification purposes only or as appropriate)

The list above is representative of many Counties, but is not necessarily the exact representation in each County. The idea is to bring in representation and buy-in from key stakeholders, management who have budget and policy authority, technical staff who know what can and cannot be supported, and legal counsel who know the legal ramifications of various policy choices. In some Counties, it may be appropriate to include Internal IT audit personnel. Involving this group is important if resulting policy statements are to reach the broadest possible acceptance. It is also relevant to mention that the role of legal counsel will also vary from county to county.

What Makes a Good Information Security Policy?

The characteristics of good information security policies are:

- They must be able to be implemented through both technical and non-technical procedures, publishing of acceptable use guidelines, or other appropriate methods.
- They must be enforceable with security and management tools, where appropriate, and with sanctions, where actual prevention is not technically feasible.
- They must clearly define the areas of responsibility for users, administrators, and management.

Countywide information security policies include the following subject areas, at minimum:

- Acceptable Use Policy
- Business Continuity Policy
- Development Life Cycle Policy
- E-mail Policy
- Incident Response Policy
- Information Classification Policy
- Logon Banner Policy
- Master or ‘Board Level’ Policy
- Password Policy
- Perimeter Policy
- Physical Security Policy
- Privacy and Confidentiality Policy
- Remote Access Policy
- Risk Assessment Policy
- Security Awareness, Training, and Education Policy
- Software Copyrights and Licensing Policy
- Virus Protection Policy

These policies address the highest-level policy of the County, and are to include all departments whether lead by appointed or elected officials. These policies are meant to ensure that the County conducts itself in a meaningful, standard manner as a model of protecting County owned or controlled informational assets. Other policies, such as Information Technology (IT) policies, will embrace these highest-level policies and lend themselves more toward IT strategies and tactics.

Once the countywide information security policies have been established they should be clearly communicated to users, staff, and management in the manner appropriate for the County. Having all personnel sign a statement indicating that they have read, understood, and agreed to abide by the policies is an important part of the process. Finally, the policies should be reviewed on a regular basis to see if it is successfully supporting the countywide information security program requirements.

Conclusion

Like any other countywide program, executive sponsorship and support are essential for this program's success. Each county in California to supplement their Countywide Information Security Program can use the Information Security Program "Best Policies" outlined in this document (policies included were templates from Sheshunoff® State and Local Government Information Security publication). They will support the County's efforts in providing availability, integrity and confidentiality of all county controlled assets, both logical (e.g., computers) and physical (e.g., building, personnel, hardcopy) as outlined in the "Best Practices" program. These policies are also based upon industry and governmental 'best practices' and have been developed by a security forum sanctioned by the California Counties Information Services Directors Association. This document will serve every County that adopts them, in one form or other, to foster, build and maintain both effective and efficient methods to safeguard assets under county control. The policies outlined in the exhibit are considered to be the minimum number of policies required for a local government security initiative.

County government are now positioned to adopt these policies in a proactive manner, as they will allow local government to deal with newly recognized threats to the United States on Homeland Security efforts, internal and external threats, as well as ongoing threats from foreign countries, including viruses and Trojans (malicious software) that place county controlled information at risk.

Exhibit 1: Information Security Policies

Introduction

Today’s information technology offers improved communication, but also increases vulnerability. Technology allows us to communicate information in many ways, including telephone, radio, television, facsimile, and computers. Critical information is distributed across different systems, consisting of various combinations of hardware, software and networks. Network interconnections offer users the ability to communicate and share data with any other connected user anywhere in the world. This capability also allows any other user to retrieve information, sometimes in inappropriate ways.

People are increasingly dependent on information technology, so it is important to protect technology from misuse. Information technology has diversified over the years, but information-handling requirements have remained relatively consistent. People need to communicate via voice, video, paper, images, and data. Because information must be protected in whatever form it takes, it is important to consider security-related issues with paper, surface mail and even presentations at public conferences. Information security policies must then address non-technical methods of handling information.

Counties and their departments should adopt commonly accepted information security policies since they directly reflect concurrence among information security professionals. Further, these policies should be adopted without change because not to do so could introduce unforeseen risks. If desired, however, Counties and their departments can use these information security policies as a reference in developing their own policies, provided a thorough risk analysis is conducted.

Information Security Policies must apply to all employees, both permanent and temporary, and all contractors, consultants, vendors, interns, volunteers and others who use the resources that are either owned or leased by the county. Policies can address both general and specific issues, but they should be tailored to those people who will be held responsible for compliance.

Purpose

There are at least four major reasons for implementing information security policies:

- Policies set the stage for appropriate behavior and awareness of acceptable business practices;
- They help staff operate information-handling systems in a secure manner;
- They assist administrators and developers in the implementation and configuration of secure information-handling systems; and,
- They provide managers a means for determining whether new requirements are adhered to, or necessitate a change in, current policy.

Acceptable Use Policy

Issue Date:
Revision Date:

1. Policy Scope

The purpose of this policy is to outline the acceptable use of computer equipment at the County. These rules 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.

2. Policy Scope

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.

3. Policy Description

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.

Internet/Intranet/Extranet-related systems, including, but not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, Web browsing, and file transfer protocol, 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.

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.

General Use and Ownership

- 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 information stored on any network device belonging to the County.
- 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.
- Authorized individuals within the County may monitor equipment, systems, and network traffic at any time for security, network maintenance and policy compliance purpose.
- The County will conduct audits on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

- Information contained on Internet/Intranet/Extranet-related systems are either confidential or public, as defined by organization confidentiality guidelines. Examples of confidential information include, but are not limited to: medical information, employee data, vendor and bidders sensitive information, lawyer/client correspondence, specifications, and other data. Employees should take all necessary steps to prevent unauthorized access to this information.
- Authorized users are assigned accounts for their specific use based on their defined needs. Users are responsible for the security of their accounts. Passwords are provided to enable users to keep their account secure. Users are not authorized to share their passwords. Users must change their password every 90 days. System administrators are to change their account passwords at least every 45 days.
- Password-protected screensaver with automatic activation set at 10 minutes or less is required on all PCs, laptops, and workstations. Log off (control-alt-delete for Win2K users) the network when the host is unattended.
- Use encryption for information that users consider sensitive or vulnerable in compliance with established standards.
- Because information contained on portable computers is especially vulnerable, exercise special care in the handling, storage and transportation of this equipment
- 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.
- 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.
- Use 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.

Unacceptable Use

The following activities are prohibited. Appropriate management personnel may consider exemptions.

Illegal activities under local, state, federal, or international laws will be turned over to the appropriate authorities.

The lists below are by no means exhaustive but attempt to provide a framework for activities that fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Products that are not appropriately licensed 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 cannot be used on County equipment.
- 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 is strictly prohibited.
- 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.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) is prohibited.
- 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.
- Making fraudulent offers of products, items, or services originating from any County account.
- 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 in to 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.
- Port scanning or security scanning is expressly prohibited unless these are within defined job duties and specifically authorized by management.
- 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.
- Circumventing user authentication or security of any host, network, or account.
- Interfering with or denying service to any user other than the employee’s host (e.g., denial of service attack).
- 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.
- Providing information about, or lists of, County employees to parties outside the County.

E-mail and Communications Activities

- 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).
- Any form of harassment via e-mail, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging of e-mail header information.
- 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.
- Creating or forwarding “chain letters,” “Ponzi,” or other “pyramid” schemes of any type.
- Use of unsolicited e-mail originating from within the County’s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the County or connected via the County’s network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4. Enforcement

Violators of this policy may be subject to appropriate disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil.

5. Definitions

Terms	Definitions
Spam	Unauthorized and/or unsolicited electronic mass mailings.

6. Revision History

Effective Date	Employee Name	Description

Business Continuity Policy

Issue Date:
Revision Date:

1. Policy Purpose

This document defines the County's Business Continuity Planning (BCP) efforts and functions, and assigns roles and responsibilities for this effort.

2. Policy Scope

This policy applies to all business units throughout the entire County organizational structure.

3. Policy Description

To adequately address BCP, each County business unit must have a documented plan to cover these five distinct areas:

Business Impact Analysis

Identify critical business functions, define impact scenarios, and determine resources needed to recover from each impact

IT Backup and Recovery Plan

IT data backups, storage, data restore procedures, recover mission critical technology and applications at alternative site

Business Contingency Plan

How to continue business without "normal" resources

Business Recovery Plan

Recover mission-critical processes at alternative sites

Business Restoration Plan

Restore normal business functions at permanent facilities

Current copies of a department's business continuity plans will 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 plan 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.

4. Enforcement

The County's Office of Emergency Services is responsible for ensuring that each County business unit has a documented BCP.

OES will ensure that these documented plans are reviewed and updated on an annual basis.

OES will conduct an Emergency Readiness Test on an annual basis that will be designed to enable the County's business units to validate their individual BCP plans, ensure that their people are adequately trained in this BCP plan, and that inadequacies of the BCP are identified and remedied.

5. Definitions

Terms	Definitions
Business Impact Analysis (BIA)	Analysis to determine the impact that certain defined disaster scenarios would have on the business unit. These disasters could include short-term and long-term disasters. The intent of this BIA is to determine what processes and resources are needed in these disaster scenarios.
IT Backup and Recovery Plan	Related to IT system back-ups and recovery. The IT Backup and Recovery Plan is provided by the IT service provider and is developed by determining the business requirements for frequency of back-ups, retention of back-up media, plans for restoring of the back-ups, and a recovery plan for restoring back-ups in an alternate IT site.
Business Contingency Plan	Defines the processes needed to continue to offer business services to clients. In a disaster situation, decreased services may be required, however, this Business Contingency Plan lists how these services are to be provided.
Business Recovery Plan	Defines the steps required to recover from a situation that had some impact on the businesses’ “normal” functions.
Business Restoration Plan	Defines the steps required to restore the business completely from a disaster that required the business to relocate, to offer limited services, or to not provide services at all.

6. Revision History

Effective Date	Employee Name	Description

Development Life Cycle Policy

Issue Date:
Revision Date:

1. Policy Purpose

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

2. Policy Scope

This policy applies to all existing Applications, Systems and Services maintenance as well as future Applications, Systems and Services development. .

3. Policy Description

A formal Developmental Life Cycle process, projects will:

- Deliver quality applications, systems, and services that meet or exceed customer expectations when promised and within cost estimates.
- Provide a framework for developing quality and secure applications, systems, and services using an identifiable, measurable, and repeatable process.
- Establish a project management structure to ensure that each development project is effectively managed throughout its life cycle.
- Identify and assign the roles and responsibilities of all involved parties, including functional and technical managers, throughout the development life cycle.
- Ensure that development requirements are well defined and subsequently satisfied.

These goals will be achieved by:

- Establishing appropriate levels of management authority to provide timely direction, coordination, control, review, and approval of the development project.
- Ensuring project management accountability.
- Documenting all requirements (e.g., functions, laws, policies) and maintaining trace ability of those requirements throughout the development and implementation process.
- Ensuring that projects are developed within the current and planned information technology infrastructure.
- Identifying project risks early and manage them before they become problems.

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 an agency 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. The phases are:

- Plan
- Analyze
- Design
- Implement
- Support

Each phase has certain Critical Success Indicators that must be achieved to ensure a successful project. It is important that key stakeholders, including customers and security be involved in each phase of the project to ensure achievement of the Critical Success Factors.

4. Enforcement

Violators of this policy may be subject to appropriate disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil.

5. Revision History

Effective Date	Employee Name	Description

E-mail Policy

Issue Date:
Revision Date:

1. Policy Purpose

This policy defines how County e-mail communications are to be used in a professional manner for County purposes. In addition, it defines how County e-mail communications are to be secured to prevent unauthorized access, to prevent unintended loss or malicious destruction of data, and to provide for the integrity and availability of all e-mail systems.

2. Policy Scope

This policy applies to all authorized users of County email systems to include employees, contractors, vendors and other users. This policy is in effect countywide whether used on county premises or off site.

3. Policy Description

County information technology resources, including Electronic Mail are to be used for County business purposes. Procedures for incidental and non-business use of County information technology resources must be defined by each individual County Department.

Access to e-mail services is a privilege that may be wholly or partially restricted without prior notice or without consent of the user.

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.

All e-mail is subject to audit and periodic unannounced review by authorized individuals as directed by the Director of each Department. 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.

E-mail is subject to the policies concerning other forms of communication as well as all other applicable policies including, but not limited to, confidentiality, conflict of interest, general conduct and sexual harassment.

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.

County Departments shall take appropriate steps to protect all e-mail servers from various types of security threats as follows:

- Place e-mail servers in safe locations that are physically secured. See the “Physical Security” policy for more information.
- Back-up the e-mail servers for software and data on a regular basis. See the “Business Continuity” policy for more information.

- Run anti-virus software on the e-mail servers to protect the server itself and all the e-mail messages that traverse through it. Apply the same security guidelines to the e-mail servers as to the other County e-mail servers.
- All County Departments must have appropriate procedures in place to monitor personnel having administrative access to e-mail servers.

County Departments shall develop policy regarding the use of Internet based e-mail services such as hotmail, AOL, yahoo, etc. Such policy 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 such as Hotmail, AOL, Yahoo, etc. where the County has no jurisdiction.

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

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 email and understand that it may be passed beyond the intended recipient. Encryption must follow County standards.

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

4. Enforcement

Violators of this policy may be subject to appropriate disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil.

5. Definitions

Terms	Definitions
Remote access	Access from locations that are removed from county premises not directly connected to the County LAN/WAN.
Strong Authentication	The process of authenticating users through the user through the use of more than one authentication factor (Possession, knowledge, biometrics).

6. Revision History

Effective Date	Employee Name	Description

Incident Response Policy

Issue Date:
Revision Date:

1. Policy Purpose

This policy outlines 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 policy be followed when responding to security incidents.

2. Policy Scope

This policy applies to all authorized users of County computerized systems to include employees, contractors, vendors and other users. This policy is in effect countywide whether used on county premises or off site.

3. Policy Description

Notify the Information Security Representative (ISR) for the department immediately of any suspected or real security incident. If the ISR 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 ISR should be contacted to evaluate the situation.

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

4. Policy Responsibilities

Individual Users:

- Report any perceived security incidents to the departmental ISR.

ISR:

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

CIRT:

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

Chief Information Security Officer (CISO):

- Review Security Incident Reports.
- Compile and maintain security incident statistics.

5. Enforcement

Violators of this policy may be subject to appropriate disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil.

6. Definitions

Terms	Definitions
CISO	County Information Security Officer

7. Revision History

Effective Date	Employee Name	Description

Information Classification Policy

Issue Date:
Revision Date:

1. Policy Purpose

This policy defines how information is to be classified. The information covered in this policy includes, but is not limited to, information that is either stored or shared via electronic means or in hardcopy form. Information and application owners, as well as other employees, should familiarize themselves with the information classification policy.

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

2. Policy Scope

All information is categorized into two main classifications:

- Public
- Sensitive

Public information is defined by the California Public Records Act, and is contained within California Government Code 6254.9.

Sensitive information is any information not declared by law or policy to be public information. Sensitive information includes the following:

- Restricted Data
- Private or Confidential Data
- Protected Data
- Intellectual Property

The Information Owner is the classification authority. It is the responsibility of the Chief Information Officer or IT Director and/or designee to apply appropriate measures to protect electronically processed and stored information so classified by the owner of that information.

3. Policy Description

Follow the guidelines below on how to classify information at varying levels

3.1 Public Records. According to California Government Code §6254.9: (a) Computer software developed by a state or local agency is not itself a public record under this chapter. The agency may sell, lease, or license the software for commercial or noncommercial use. (b) As used in this section, "computer software" includes computer mapping systems, computer programs, and computer graphics systems. (c) This section shall not be construed to create an implied warranty on the part of the State of California or any local agency for errors, omissions, or other defects in any computer software as provided pursuant to this section. (d) Nothing in this section is intended to affect the public record status of information merely because it is stored in a computer. Public records stored in a computer shall be disclosed as required by this chapter. (e) Nothing in this section is intended to limit any copyright protections.

3.2 Non-Sensitive Information. Non-sensitive information is considered public information. This is information that 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 for direction.

3.3 Sensitive Information. Sensitive information can be broken down into other classifications: restricted, private or confidential, protected, and intellectual property. Sensitive information includes 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, telecommunications, and systems. Information that is covered by non-disclosure agreements or intellectual property practices is considered sensitive information.

a. Restricted Data. Examples of restricted information include CLETS, Medical Examiner/Mortician, 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:

- Computer readable files
- Reports and Printouts
- Terminal and Monitor displays
- Program Source and Object code
- Systems and Program documentation
- User documentation

b. 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:

- Passwords
- Personal medical condition or related information
- SSN
- Personal or family information

- Family names
- Ages
- Personal or business partner financial and banking data, including credit cards, bank routing numbers and bank account information
- 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)
- County financial data not deemed public by the Public Records Act
- Employee performance reviews, discipline reports and other personnel data,
- Information related to in progress legal proceedings
- The combination of a logical address, User ID, and password
- 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.

c. 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:

- Telecommunications and cabling schematics
- Disaster Recovery Plans
- Operational Recovery Plans
- Network schematics
- Physical facility schematics
- Preliminary reorganization plans
- Detailed information about ongoing projects
- Time sensitive information
- Risk assessments
- System controls

Only County personnel with a designated need-to-know are 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, however, managers must always obtain Department information owner consent before granting access or releasing protected information.

d. Intellectual Property. Without specific written exceptions, all programs and documentation generated by, 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.

4. 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 designee(s) 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 <responsible organization> to assure that facility security needs of sensitive information are met.

5. Declassifying or Reclassifying Information

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.”

6. Enforcement

Violators of this policy may be subject to appropriate disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil.

7. Definitions

Terms	Definitions
Access	Making information available to only those individuals with a business need to know – requires authorization by the Information Owner and signed Ethics and Responsible Use and Non-Disclosure Agreements.
Distribution within	Access within the owning department or other County entity with a business need to know via and electronic file

	transmission methods.
Distribution outside	Access outside of the County to approved parties with a business need to know via public or private carriers and approved electronic file transmission methods.
Information Owner	The Department Head and/or designee assigned responsibility under State or federal law or County policy for specific data, including classification, protection and assigning access.
Intellectual Property	Documentation, software, code, copyrights, inventions or patents to which the County or a third-party has legal ownership, and therefore maintains exclusive rights.
Non-Sensitive Information	Non-sensitive information is considered public information.
Private or Confidential Data	A category of Sensitive Information. County-held information requiring defined access and distribution controls.
Protected Data	A category of Sensitive Information. Information that may be deemed public by the Public Records Act, but if made available through public media could create vulnerabilities for the County.
Public Information	Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to the County or its customers and/or business partners.
Restricted Data	A category of Sensitive Information. Information that by law requires strict access and distribution control. State and Federal laws and regulations that place stringent privacy and security requirements on some or all of the data prescribe protection measures.
Sensitive Information	Sensitive information is any information not declared by law or policy to be public information.

8. Revision History

Effective Date	Employee Name	Description

Logon Banner Policy

Issue Date:
Revision Date:

1. Policy Purpose

The purpose of this policy is to warn users of their responsibilities when accessing County network and computer systems.

2. Policy Scope

This policy applies to all County employees, contractors, consultants, temporaries, and other workers, including all personnel affiliated with third parties.

3. Policy Description

This document establishes County policy that all communications equipment 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 that access is for official use only.

The following banner contains all the necessary elements (see Background below). This should be considered as the County standard logon-warning banner.

> **"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!"***

Background:

In general, legal opinion is that people have to be aware of limitation and penalties before they can be held accountable. Therefore, to establish a reasonable expectation that users 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 needs to establish a Logon Banner that notifies users of these limitations. The Department of Justice has made the following recommendations on what should be included in such a warning.

- 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).
- People must be advised that they are subject to having their activities monitored and that use of the system implies consent to such monitoring. They also need to know that information gathered may be given to law enforcement or other investigative officials for action if warranted.

- They need to be aware of the impact of inappropriate use/access.
- They must acknowledge this warning by some positive action on their part, like a keystroke.

Monitoring:

Users should be made aware that their actions might be monitored. The following is an example of the 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."

4. Enforcement

Violators of this policy may be subject to appropriate disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil.

5. Definitions

Terms	Definitions

6. Revision History

Effective Date	Employee Name	Description

County Information Security Policy

Issue Date:
Revision Date:

1. Policy Purpose

The purpose of this policy is to define a countywide policy for the appropriate access to and integrity of County information and information technology assets.

2. Policy Scope

The County Information Security policy serves as the minimum standard to which all Departments must adhere. Additional subordinate policies addressing specific areas of information security also exist. Individual Departments may implement additional information security policies to meet their business needs but cannot establish policies that would supercede countywide policies.

3. Policy Description

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 (IT) assets which are 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 policies and procedures. The Department Head will ensure the appointment of a Departmental Information Security Representative (ISR) to be responsible for managing information security within the Department. This person will represent the Department in the area of information security.

Departmental Information Security Representative (DISR) will:

- Manage information security within the department
- Be responsible for any Departmental information security policy
- Represent Department in the Countywide Information Security Committee
- Coordinate the Departmental Computer Emergency Response Team (DCERT)

Employees and Authorized Users

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

Chief Information Security Officer (CISO)

The Chief Information Security Officer will:

- Chair the Countywide Information Security Advisory Committee (ISAC);
- Provide information security related technical, regulatory, and policy leadership;
- Facilitate the implementation of County information security policies;
- Coordinate information security efforts across departmental lines;
- Lead continuing information security training and education efforts;
- Serve as an information security resource to Department Heads and the Board;
- Represent the County at professional information security forums and State and Federal events related to information security; and
- Report to the appropriate authority (CAO, BOS or CIO).

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 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.

ISAC responsibilities will be to:

- Develop, review, and recommend information security policies
- Develop, review, and approve best practices, standards, guidelines and procedures
- Coordinate Inter-Departmental communication and collaboration;
- Coordinate Departmental information security education and awareness;
- Recommend appropriate hardware and software.

4. Enforcement

Violators of this policy may be subject to appropriate disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil.

5. Definitions

Terms	Definitions
ISR	Information Security Representative responsible for guiding the countywide information security efforts, and implementation within their departments.
ISAC	Information Security Advisory Committee established to provide departmental input and advice related to county security initiatives.

6. Revision History

Effective Date	Employee Name	Description

Password Policy

Issue Date:
Revision Date:

1. Policy Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

2. Policy Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any County facility, has access to a County network, or stores any County controlled information.

3. Policy Description

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.

4. Policy

4.1. General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a monthly basis.
- All production system-level passwords must be part of the security administered global password management database.
- All user-level passwords (e.g., e-mail, applications, Web, desktop computer, etc.) must be changed at least quarterly. The recommended change interval is every two months.
- 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.
- Passwords must not be inserted into e-mail messages or other forms of electronic communication.
- Where 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).
- All user-level and system-level passwords must conform to the guidelines described below.

4.2. Policy Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at the County. Some of the more common uses include: user level accounts, Web accounts, e-mail accounts, screen saver protection, voicemail password, and local router log-ins. Since very few systems have support for one-time tokens (i.e., dynamic passwords that are used only once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters.
- The password is a word found in a dictionary (English or foreign).
- The password is a common usage word, such as:
- Names of family, pets, friends, coworkers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software
- The word <county name> or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z).
- Have digits and punctuation characters as well as letters, e.g., (0-9, !@#$%^&*()_+|~-=\`{}[]:”;’<>?,./). (Note: not all systems allow for the use of these characters).
- Are at least eight alphanumeric characters long.
- Are not a single word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down (unless store in a locked safe for recovery purposes) or stored online. Try to create passwords that can be easily remembered yet hard to guess. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, 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!**

B. Password Protection Standards

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.). Where possible, don’t use the same password for various County access needs. For example, select one password for the network systems and a separate password for application systems. Also, select a separate password to be used for a NT account and an AS400 or UNIX account.

Do not share County passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential County information.

Here is a list of things to avoid:

- Giving your password over the phone to ANYONE.
- Sending a password in an e-mail message.
- Telling your boss your password .
- Talking about a password in front of others.
- Hinting at the format of a password (e.g., “my family name”).
- Writing in your password on questionnaires or security forms.
- Sharing your password with family members.
- Telling your co-workers your passwordwhile on vacation.

If someone demands a password, refer him or her to this document or have him or her call someone in Information Security.

Never use the “Remember Password” feature of applications (e.g., Eudora, Outlook, Netscape Messenger).

If you must your passwords down, store them is a secure place and never anywhere in your office.

Passwords stored in a file on ANY computer system (including Palm Pilots or similar devices) can be compromised if encryption isn’t used to secure them.

Change passwords at least once every three months (except system-level passwords, which must be changed monthly). Changing them more often is better.

If you suspect that your account or password is compromised, report the incident per the Incident Response Policy and change all passwords.

Password strength checking may be performed on a periodic or random basis by departmental or county IT or its delegates. Any passwords found out during one of these scans will require the user to change it.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications should:

- Support authentication of individual users, not groups.
- Not store passwords in clear text or in any easily reversible form.
- 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.
- Support TACACS+, RADIUS, and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users

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.

E. Pass phrases

Historically pass phrases have been used for public/private key encryption. However, there is no reason that pass phrases can't be used as a more secure version of a password. A pass phrase is composed of multiple words. Because of this, a passphrase is more secure against password "dictionary attacks."

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!"

All of the rules above that apply to passwords apply to passphrases.

5. Enforcement

Violators of this policy may be subject to appropriate disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil.

6. Definitions

Terms	Definitions
Application administration account	Any account that is for the administration of an application (e.g., Oracle DBA, RACF administrator).
SNMP	Simple Network Management Protocol.
TACACS+	Terminal Access Controller Access Control System.
RADIUS	Remote Authentication Dial-In User Service.
X.509	The most widely used standard for defining digital certificates.
LDAP	Lightweight Directory Access Protocol.
RACF	Resource Access Control Facility.

Revision History

Effective Date	Employee Name	Description

Perimeter Policy

Issue Date:
Revision Date:

1. Policy Purpose

This policy defines the Security Perimeter and its supporting architecture. Furthermore, it establishes the core strategies, essential policies and operational requirements regarding the management and maintenance of the Security Perimeter and its supporting architecture.

2. Policy Scope

The Security Perimeter is an essential and critical Wide Area Network component and crucial to the security of County infrastructure information systems.

This policy applies to all resources, systems, connectivity, and services as defined within the Security Perimeter and to all entities located on the County Wide Area Network. This policy will not supercede existing legal requirements..

3. Policy Description

The Security Perimeter is defined as all resources, systems, connectivity, and services responsible for enabling and maintaining connectivity between an organization, its business partner(s), and all other external-to-organization resource(s) or service(s). It represents the "managed point of entry/exit" to County infrastructure resources. It includes but is not limited to Firewalls, Intrusion Detection Systems (IDS), Demilitarized Zones (DMZ's), remote connectivity resources, and the network architecture resources providing connectivity for the environment.

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

- **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 configures) services will be available. All other unused services are denied.

- **The Principle of Least Privilege**

  The principle of least privilege states that an object (host, service, resources, subnet, etc) should have the minimum privileges necessary to perform its assigned task and no more.

- **Minimize Publication of Information**

  Best business practice and strategy to minimize the amount of internal network resource information that is disclosed to trusted and non-trusted entities.

- **Single Entry/Exit**

  Best business practice and strategy to have a single point of entry to the Wide Area Network or Intranet. (While this, dependent on organization, may not be achieved physically it is critical that logically security standards are applied uniformly across the defined Security Perimeter).

- **Principle of Accountability and Responsibility**

  The principle that to be accountable for security one must be responsible for the resources that maintains it.

In accordance with these strategies the following policy 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).

Authority

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

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.

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.

- **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.
- **External Auditing:** Periodic auditing, which assess the efficiency and accuracy of internal auditing and performed by individuals, groups, or third parties not involved with the Security Perimeter.
- **Vulnerability Assessment:** The regular execution of vulnerability identification measures which include both internal and external assessments, and assessments by bonded external third parties.

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 policy statements apply.

Any external connection to or from the County Wide Area Network must come through the security perimeter's managed point of entry.

Only authorized outbound services will be initiated from internal County hosts to external-to-County hosts as approved by the CA.

The CA will approve inbound services on a case by case.

Extranet partners connecting to County resources cannot use the County as a conduit for connectivity to each other.

Any entity connecting to the County, shall sign all necessary security and confidentially agreements.

Logging

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

- 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.
- The integrity of system logs must be protected with checksums, digital signatures, encryption, and/or similar measures.
- System logs removed or recorded from its associated system must be done so in a secure manner to ensure the admissibility in court.
- System logs must be reviewed to ensure that the Security Perimeter is operating in a secure manner and to detect anomalous activity.
- Any anomalous activity indicating or suspected of indicating unauthorized usage or access must also be documented according system procedures.

Remote Access

Remote Access refers to remote access connectivity such as dial-up networking and/or Virtual Private Networking (VPN) that is utilized to gain privileged access to County Infrastructure systems.

- In accordance with external connectivity policy, all remote access connections must come through the Security Perimeter.
- 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).
- Remote access sessions will be monitored and logged and employ session time limits (active idle).
- Remote access sessions utilizing the Internet as the means of connectivity must be encrypted in accordance with standards approved by the CA

- Remote access sessions connecting to County networks and resources in all instances possible, must involve extended user authentication (single to multifactor authentication) measures approved by the CA.

Information Sharing and Publication

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

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

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:

- Deployment of dedicated Firewall technologies.
- Deployment of Demilitarized Zones (DMZs) for resource hosting (i.e., Internet/Extranet accessible resources) and access filtering.
- Deployment of Network Intrusion Detection Systems (NIDS) on all capable segments (Protocol Anomaly Detection (PAD) and signature detection capable).
- Deployment of Host Intrusion Detection Systems (HIDS) on all capable hosts.
- Virus screening resources on all necessary entry points.

Security Perimeter Resource Security

Access to resources within the security perimeter must be provided in a manner that adheres to the strategies of Least Privilege and the Principle of Accountability and Responsibility. To this end the following statements apply:

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

Security 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 policy statements apply:

- 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.
- All resources within the Security Perimeter must employ all necessary security patches and security configurations in a timely manner as determined by the CA. In instances where this is not possible, due to system in compatibility or patch failure, the CA must approve this action through appropriate risk assessment procedures.
- To the degree possible, all maintenance patches and configuration must be tested prior to implementation.
- As monitoring introduces potential security risks, local and remote, will only be authorized in a manner approved by the CA. As security needs change, monitoring capabilities may also change.
- Administrators of Security Perimeter must have access to or receive notification from vulnerability advisory bodies (CERT, etc) and be responsive to applicable vulnerabilities.

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.

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

4. Enforcement

Violators of this policy may be subject to appropriate disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil.

5. Definitions

Terms	Definitions

6. Revision History

Effective Date	Employee Name	Description

Physical Security Policy

Issue Date:
Revision Date:

1. Policy Purpose

This policy describes the responsibilities for protecting physical computer and information resources, including non-computer informational assets.

2. Policy Scope

This policy applies to all county information and information systems assets.

3. Policy Description

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

4. Policy Responsibilities

Director/CIO of Information Systems:

- Identify and enforce physical security requirements.
- Identify requirements for environmental protection of the computer center and any remote facilities.
- 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.
- Maintain and keep current, an inventory of physical computer and information resources including peripherals.
- Maintain and keep current a list of authorized service vendors entering the computer center for repair and maintenance of equipment.
- Authorize a County escort for any person whose access to the computer center is not a job requirement.

Information Systems Employees:

- Report the loss or theft of an information resource to management and complete required forms, if any.
- Notice suspicious individuals (e.g., maintenance, public and others visiting the organization, delivery personnel, vendors, etc.) and be prepared to challenge individuals entering the computer center or other restricted areas.
- Inventory and store data file backup information at an off-site location per established retention schedules.

Users:

- Secure information resource equipment in their possession at all times while on site or in possession.
- Report the loss or theft of an information resource to management immediately and complete required forms, if any.
- Challenge any persons or activities unknown to you or that appear to not belong at that physical location.
- Ensure proper disposal of an information asset based upon departmental, local, state, or federal law or rule.

Security Administrator:

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

Internal Auditor:

- Audit the computer center to determine compliance with the above policy.
- Review physical security considerations and recommend appropriate controls.
- Evaluate the effectiveness of environmental controls.

5. Enforcement

Violators of this policy may be subject to appropriate disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil.

6. Revision History

Effective Date	Employee Name	Description

Privacy and Confidentiality Policy

Issue Date:
Revision Date:

1. Policy Purpose

This policy outlines the steps required to safeguard or release non-public, County computer-based information.

2. Policy Scope

This policy applies to all information that exists with the county environment, either owned by or in the custody of the county.

3. Policy Description

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

Responsibilities

Director of Information Systems/CIO:

- Provide encryption capabilities of information that is deemed highly confidential (i.e., wire transfers) as directed by the information owner.
- Remove information from data storage and memory of computer equipment prior to sending such equipment for maintenance, salvage, or redeployment.
- Protect software and data/information by including a nondisclosure agreement with outside professional services contracts.

County Users/Information Systems Employees:

- Protect information resources against unauthorized access, loss, or destruction.
- Keep nonpublic information confidential.
- Retain information solely for legitimate business purposes.
- Retrieve confidential or restricted documents immediately from fax, printers, or copy machines.
- Shred printed nonpublic data/information prior to disposal.
- Secure access codes and information (i.e., dial-up phone number, passwords).
- 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.

Information Security Representative:

- Investigate reports with data/information suspected of illegal tampering.
- Inform users about the reasons data has to be protected, legislation that affects their work, and other topics within the Information Security Policies.

4. Enforcement

Violators of this policy may be subject to appropriate disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil.

5. Definitions

Terms	Definitions

6. Revision History

Effective Date	Employee Name	Description

Remote Access Policy

Issue Date:
Revision Date:

1. Policy Purpose

To establish policy for allowing only authorized access to the County's computer network from a location that is not physically connected to the County network (remote site).

2. Policy Scope

This policy applies to all County employees (permanent and temporary), elected officials, contractors, consultants, non-County agencies, and others who are authorized to access the County's computer networks.

The policy also applies to all computer and data communications systems administered by the County or for the County by authorized IT service providers.

3. Policy Description

Remote access is granted for authorized County work only.

- 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).
- Internet services will be strictly controlled by firewall technology to provide preventative and detective controls.
- Access from a remote site to a County network that contains SENSITIVE or RESTRICTED information (as defined in the Acceptable Use policy) requires extended identification and authentication procedures.
- 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.
- When an authorized user terminates County employment or transfers to another County department, office or agency, all existing remote access services will be terminated. 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.

4. Policy Responsibilities

Responsibility for implementation of this policy is as follows:

CAO / CTO Responsibilities:

- Ensure that policy documents and associated guidelines for remote access usage reflect the County's mission, goals, and values.

IT Responsibilities:

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

Departmental Responsibilities:

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

End-user Responsibilities:

- Follow County and departmental policies, practices, and guidelines as they relate to remote access.
- Follow County and departmental policies regarding information disclosure.

5. Definitions

Terms	Definitions

6. Revision History

Effective Date	Employee Name	Description

Risk Assessment Policy

Issue Date:
Revision Date:

1. Policy Purpose

The purpose of this policy is three-fold. First, the policy identifies and authorizes individuals charged with responsibility of assessing risk. Secondly, it identifies the security policies and procedures to be enforced in order to initiate appropriate remediation. Lastly, it requires the performance of periodic information security risk assessments for the purpose of determining areas of vulnerability.

2. Policy Scope

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.

3. Policy Description

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 policy 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 requires full cooperation. It is the joint responsibility of the Risk Assessment Authority and those responsible for the area being assessed to perform effective remediation.

Furthermore;

- The Chief Information Security Officer (CISO) or CISO's designee(s) 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.
- 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.
- All Risk Assessment findings will be documented and confidential to the necessary parties identified at Risk Assessment commencement.
- The activities of Risk Assessment Authorities will not be compromised.
- Identified vulnerabilities will be assessed for criticality. All vulnerabilities that unnecessarily endanger or expose resources must be immediately remediated.
- All vulnerabilities identified for remediation must be reported to and acknowledged by the CISO or the CISO's designees.

4. Policy Enforcement

Violators of this policy may be subject to appropriate disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil.

5. Definitions

Terms	Definitions
Entity	Any business unit, department, group, or third party, internal or external to, responsible for maintaining assets.
Risk Assessment Authority	Individuals designated with the authority to conduct Risk Assessments.
Risk	Those factors that could affect confidentiality, availability, and integrity of key information assets and systems. Risk Assessment Authorities are responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.

6. Revision History

Effective Date	Employee Name	Description

Security Awareness, Training, and Education Policy

Issue Date:
Revision Date:

1. Policy Purpose

Security Awareness Training & Education (SATE) is key to eliminating the County's exposure to both malicious threats and accidental errors and omissions. SATE is not only defined as industry best practices, it is also a statutory requirement. This policy sets forth a minimum standard for SATE to reduce the County's 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.

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

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

2. Policy Scope

This policy applies to all Employees (regular full time and part time, represented and unrepresentative employees and extended staff contractors). The level of SATE required by an individual employee is determined by that employee's level of access to information and information systems. Some employees will require more SATE than others. Roles and responsibilities must be clearly defined and communicated in this training.

3. Policy Description

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.

Most County employees will only need the minimum level of security training as follows:

- Incorporate basic security training for all new hires, ideally before a new hire sits down to do his or her job;
- Include in the training curriculum "social engineering" techniques that hackers use to gather information;
- All employees must attend security policy training classes every two years;
- All employees must be tested for basic security awareness every year;
- Explain to employees that while their departments are the "owners" of the data, they need to assist the Information Systems department in its safekeeping;
- Explain to employees the difference between "public" records and the need to keep information "confidential;"
- State reasons why specific policies are needed;
- Describe what is covered by the policies;
- Define policy contacts;

- Define user's responsibilities;
- Define how violations will be handled.

Certain employees, including but not limited to Information Security employees and Information Technology employees will require more frequent and in-depth training due to their high level of access to information.

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.

Following are some basic elements needed to increase security awareness:

- Pre-Login "Splash Screen" with usage warning. Must point to the county's Acceptable Usage documentation;
- Posters and emails;
- Web sites;
- Periodic meetings, contests, and positive reinforcement;
- Printable Security Newsletter available from Intranet security web site.

4. Enforcement

Violators of this policy may be subject to appropriate disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil.

5. Revision History

Effective Date	Employee Name	Description

Software Copyrights and Licensing Policy

Issue Date:
Revision Date:

1. Policy Purpose

To establish a countywide policy that follows the law concerning software copyrights and licensing to helpreduce the potential financial liability to the County.

2. Policy Scope

This policy applies to all authorized users of County-owned or leased computer equipment.

3. Policy Description

Use only legally acquired and licensed software.

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

Only software that has been legally acquired and licensed may be used. 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 insure that they have valid licenses for all software used in their department.

Outside software must be authorized.

There is a 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.

4. Enforcement

The County retains the right to examine all electronic storage media, data files, logs and programs used on County computer equipment. This policy is intended as a starting point and may be enhanced by your department to cover any special circumstances.

Violators of this policy may be subject to appropriate disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil.

5. Definitions

Terms	Definitions
Copyright	The exclusive legal rights to publish, reproduce, copy, or sell the matter and form. If a work is copyrightable, it should be treated as if it is protected by copyright.
License	Authorization by the owner of a work permitting the use of that work.

6. Revision History

Effective Date	Employee Name	Description

Virus Protection Policy

Issue Date:
Revision Date:

1. Policy Purpose

All County PCs (desktop, laptop, hand-held devices) and servers are to maintain active virus protection according to the responsibilities described within this policy.

2. Policy Description

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 (specifically, e-mail attachments), and documents downloaded from the Internet. A virus infection is almost always costly to the County whether through the loss of data (possibly permanent); staff time to recover a system, or the delay of important work.

At the County, computer viruses impact the County as a whole and not just infected systems in a specific department. This is the case because 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.

3. Policy Responsibilities

Information Technology Responsibilities

- Define an enterprise anti-virus solution and negotiate a volume purchase for the County as a whole.
- Architect and monitor the overall design, function, and effectiveness of the anti-virus protection systems throughout the County.
- Inform departments of recommended operating system and application patches that are required to protect against potential system security problems.
- Provide guidelines on installing and maintaining the anti-virus software and pattern file updates on departmental servers and workstations.
- Set up "primary" 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.
- 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.

Department Responsibilities

- Ensure that all departmental file and print servers and all workstations have current anti-virus software installed.
- Ensure that once installed, anti-virus software is not disabled on servers or workstations.
- Perform day-to-day administration of their anti-virus servers.
- Configure departmental anti-virus servers such that staff can remotely verify that the servers are operational and utilizing the most recent virus protection pattern.
- Train users on the use of anti-virus software on the desktop.
- Apply any recommended operating system and application patches to protect against potential system security problems.
- Notification of any virus or network security-related incidents.
- Designate a primary and an alternate coordinator who can be contacted and is able to participate in the event of a significant virus incident.

Individual User Responsibilities

- Exercise caution when opening email attachments. Users should not open attachments that they do not expect or from users they do not know.
- Exercise extreme caution when downloading files from the Internet. Files should only be downloaded from reputable sites.
- Report virus incidents to their departmental IT staff and, if known, provide them with the following information: (1) the name of the parties involved (e-mail received from, or infected file on a server, etc.), (2) virus name or type, and (3) source of virus (e-mail, Internet download, floppy diskette, etc.).
- 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.
- Follow the appropriate policies and keep personal use of County equipment to a minimum to reduce the possibility of receiving virus-infected e-mail on County equipment.

4. Enforcement

Violators of this policy may be subject to appropriate disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil.

5. Revision History

Effective Date	Employee Name	Description

References

Wherever possible, policies should refer to original sources. For example, a policy on "hardening" web servers should refer to the manufacturer’s documentation in case a new vulnerability is discovered that changes the recommendation. Existing laws, regulations and agreements must not be superceded by policies unless exceptions are allowed.

The following sources are highly recommended for helping develop information security policies:

ISO 17799.

“Common Body of Knowledge” International Information Systems Security Certification Consortium, Inc. 2001.

Charles Cresson Wood. “Information Security Policies made Easy” Baseline Software. 1997. ISBN 1-881585-01-8.

Sheshunoff® State and Local Government Information Security.

Michele Guel. “Proven Practices for Managing the Security Function.”

www.sans.org/rr/policy- The site contains articles and papers written by GIAC certified professions.
http://www.ietf.org/rfc/rfc2196.txt?Number=2196 - The Site Security Policies Procedure Handbook.
http://www.securityfocus.com/data/library/Why_Security_Policies_Fail.pdf

Some general websites with information security policies:

http://www.security.kirion.net/securitypolicy/
http://www.network-and-it-security-policies.com/
http://www.brown.edu/Research/Unix_Admin/cuisp/
http://iatservices.missouri.edu/security/
http://www.utoronto.ca/security/policies.html
http://irm.cit.nih.gov/security/sec_policy.html
http://w3.arizona.edu/~security/pandp.htm
http://secinf.net/ipolicye.html
http://ist-socrates.berkeley.edu:2002/pols.html
http://www.ruskwig.com/security_policies.htm
http://razor.bindview.com/publish/presentations/InfoCarePart2.html
http://www.jisc.ac.uk/pub01/security_policy.html