San Mateo County
INFORMATION TECHNOLOGY SECURITY POLICY

Policy revised on: March 24, 2003

I. Introduction

Overview

This policy outlines the proper use of Information Technology resources owned or operated by the County of San Mateo and establishes standards for the base configuration and operation of those resources. The policy applies to employees, contractors, consultants, temporary and other workers at County offices, including all persons affiliated with third parties. The policy applies to all computer equipment and related devices owned or operated by San Mateo County, to all computers and communications devices not owned or operated by the County that are present on San Mateo County premises and to computers and communications devices that remotely access the County's internal network. It includes all software, firmware and other elements of those devices and their interconnections. Effective implementation of this policy will help protect the integrity of the County's network and minimize unauthorized access to information residing on the network.

Due to the rapidly changing nature of technology and its impact on the workplace the Chief Information Officer will review this policy annually and recommend any necessary changes to the County Manager. The Chief Information Officer is responsible for maintaining documentation of all variances to this policy and reporting variances to the County Manager annually. Department Heads are responsible for advising the Chief Information Officer of all situations that require deviation from or exception to this policy.

Effective security is a team effort involving the participation and support of every County employee and affiliate who deals with County information and/or information systems. It is the responsibility of all County Departments to insure that their employees are familiar with this policy. It is the responsibility of every computer user to conduct their activities accordingly. Use of County information systems constitutes consent to this policy.

Definitions

The following terms have the meanings indicated below unless the context indicates otherwise.

County Network	As used here "County network" includes the County's information network backbones, department Local Area Networks and all devices that attach, directly or indirectly, to the networks including remote attachments.
Employees	As used here "employees" include all County employees as well as temporary and other workers and all contractors, consultants, vendors, and business affiliates, including persons affiliated with third parties who operate computer equipment on behalf of the County or operate computer equipment that remotely access the County's internal network.
Users	Synonymous with employee
Chief Information Officer	As used here "Chief Information Officer", or his designee, is the County's Information Technology Security Officer. In this capacity the Chief Information Officer is responsible for implementing

	security policy, issuing security alerts, documenting security incidents and reporting to executive management on the state of information security in the County.
Department of Information Services	As used here "Department of Information Services" generally refers to the Communications Division within the Department of Information Services. The Communications division is responsible for the maintenance and County's information network backbone.
Information Services Department	Synonymous with Department of Information Services

Other County Policies

The County has other policies that may address specific areas of information security including policies on Internet use, Email and portable computing. Departments may have internal policies that also address information security issues. These policies are cumulative and in the event of conflict the policies providing the County with the greatest level of security apply.

II. User Responsibility and Acceptable Use

The purpose of this section is to outline the acceptable uses of the County's computer equipment and detail some of the prohibited and inappropriate uses. Inappropriate use exposes the County to risks including virus attacks, compromise of network systems and services, and legal issues. The lists are not exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

User Responsibility

1. Users are responsible for protecting any information used or stored in their San Mateo County accounts or equipment and any information within their area of work responsibility.
2. Users are responsible for reporting any security breaches or weaknesses they become aware of to their supervisors and department Information Technology support staff.
3. All documents and other data created or maintained by users should be saved on network drives, rather than local drives, unless directed differently by department Information Technology support staff or as required by government regulation.
4. All unsolicited Email should be treated with suspicion; particularly Email received from the Internet. If the user is unsure of the authenticity and integrity of an Email it should be referred to department Information Technology staff or deleted.

Requests for Information

Targeted attacks on corporate information resources often begin with the acquisition of key information through deceit, using deceptive interactions with trusting employees of the targeted enterprise. This information is later used as the cornerstone of technical attacks on the enterprise. Protecting the County from attacks of this nature is the responsibility of every County employee.
Users must not divulge details or instructions regarding passwords, remote access, including external network access points or dial-up numbers unless the following conditions have been met.

1. The requester has been positively identified.
2. The requester's authorization to receive the requested information has been verified.
3. Providing of the information is within the job responsibilities of the information provider.

Internal information not designated as Public information is to be shared only within the County or with authorized persons. Prior to releasing any information that is not designated as Public over the telephone, the person releasing the information must personally recognize the requester's voice through prior business contact or verify that the call is being made from an internal telephone number that has been assigned to the requester.

Prohibited Activities and Inappropriate Uses of Information Technology

The following activities are prohibited except when necessary to fulfill legitimate job functions.

1. Creating security breaches including, but not limited to, unauthorized access, alteration, destruction, removal and/or disclosure of data, information, equipment, software or systems.
2. Creating disruptions of network communication including, but not limited to, pinged floods, packet spoofing, denial of service, and forged routing information
3. Port scanning, security scanning, network sniffing or SNMP monitoring unless authorized by the Chief Information Officer. Port scanning within assigned department network segments is authorized for department Information Technology staff.
4. Circumventing user authentication or security of any workstation, terminal device or account.
5. Deliberate over-extension of the resources of a system or interference with the processing of a system.
6. Installing software on County computers that is not authorized by the user's department.
7. Adding unauthorized hardware devices that may compromise the integrity of the network, including, but not limited to, modems, FAX cards and unauthorized wireless access points.
8. Downloading, installing or running any programs or services that provide ongoing communications with the Internet which have not been approved by the Chief Information Officer, including but not limited to instant messengers, screen savers, peer to peer communications such as Kazaa and all streaming media.

9. Using County computers and resources for commercial purposes, personal gain, political campaigns or activities that are not compatible with County government.
10. Using a County computing asset to generate, send, request, receive or archive material in any form, i.e., text, graphics, etc., which contains offensive language or is harassing in nature.
11. Disclosing or requesting disclosure of confidential passwords, personal identification numbers and/or access devices or information for accessing accounts, equipment, and telephone voice mail.
12. Any use that violates federal, state or local laws.

Privacy of Personal Data

While the County desires to provide a reasonable level of privacy for employees, users should be aware that all data on County systems is the property of the County. Because of the need to protect the County network, the confidentiality of personal information stored on any network device belonging to the County cannot be guaranteed. County employees have no right or expectation of privacy of information stored on County information systems. The County reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

III. Password Management

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. Poorly chosen passwords may result in the compromise of the County's entire enterprise network. As such, all employees (including contractors and vendors with access to County systems) are responsible for taking the appropriate steps to select and secure their passwords. The following standards apply to all passwords that allow user access to the County network, or devices attached to the County network, and to Secure systems. The Chief Information Officer must be notified of any systems whose design prohibits complying with this section.

1. All users must have unique account IDs that identifies a single account owner.
2. User account names and passwords must not be the same.
3. All account IDs must have unique passwords.
4. The minimum password must contain at least is six characters.
5. At least one character in each password must be non-alpha.
6. Passwords must not contain consecutive identical characters.
7. Passwords are not to be shared, posted, or recorded except in a secure manner.
8. Passwords should change at the user's first log-on and thereafter at intervals of not more than sixty days.
9. New passwords must be unique from previously used passwords.
10. For Secure systems the minimum length password is eight characters.

For purposes of this policy Secure systems include Criminal Justice systems, Child Protective Services systems, Financial Management Systems, systems containing Protected Health Information as defined by HIPAA, passwords that remotely access the County network and all system-level passwords. The nature of data in a Secure system is such that any unauthorized disclosure would violate laws pertaining to confidentiality or could seriously impact the County, its customers or clients. Department Heads may designate other systems for which they have primary responsibility as Secure systems that will thereby be subject to the provisions of this section.

Password resets requested of support staff by telephone or Email must not be undertaken until the identity of the requester has been verified. Acceptable verification includes:

1. Personal recognition of the requester including recognition of the requester voice.
2. Call back to the requester's telephone, as listed in the County telephone directory.
3. Challenge / response keyword verification where the requester responds correctly with two pieces of pre

determined personal information.

IV. System Auditing and Configuration Standards

Auditing

Information Services

The Chief Information Officer will maintain a database of all servers on the County network including server hardware descriptions and operating system versions, physical server locations, department contact and backup contact information. The Chief Information Officer will verify the information in the server/contact database annually.

The Information Services Department will monitor network traffic as necessary and appropriate, to determine network utilization and availability and for the detection of unauthorized activity and intrusion attempts.

When a security problem, or potential security problem, is identified Information Services will seek the co-operation of the appropriate contacts for the systems and networks involved in order to resolve such problems. In the absence or unavailability of such individuals Information Services will act unilaterally to contain the problem, up to and including temporary isolation of systems or devices from the network, and notify the responsible system administrator when this is done.

All Departments

Departments should enable auditing on all production servers capable of generating audit logs. As audit logs, by default, capture large volumes of information, the logging functions should be tuned to capture only the necessary information. The logs should be reviewed on at least a weekly basis. Online logs older than one week, which do not contain suspicious data, may be purged, provided archived logs for the previous four weeks are available. The Chief Information Officer must be notified of any systems that do not have logging enabled.

Standard events to audit include:

1. User ID.
2. Date/Time of Log on/off.
3. Terminal identification.
4. Successful/rejected system access attempts.
5. Successful/rejected data and other resource attempts.

Significant computer security compromises or events should be reported to the Information Services Department who will assist in reviewing log files and other data. Information Services will assist departments in remedying the security breach, prescribing corrective measures as needed. Security-related events include, but are not limited to: port-scan attacks, evidence of unauthorized access to privileged accounts, repeated anomalous occurrences that are not related to specific applications on the host computer. Information Services will maintain a database of security incidents.

Departments will provide the Chief Information Officer the following information on any server connecting to the County network within five business days of the server being brought on line: Server hardware description and operating system version, physical server location, department contact and backup contact information.

Configuration Standards

Information Services

The Information Services Department will prepare system configuration recommendations and guidelines for network and system administrators and provide assistance and advice to the extent possible with available resources. The Chief Information Officer will publish security alerts, vulnerability notices and patches, and other pertinent information in an effort to prevent security breaches.

All Departments

Internal Servers

This section establishes the minimum standards for the base configuration of internal server equipment that is owned or operated by San Mateo County, and to servers registered under any County owned internal network domain.

1. General-purpose server operating systems for current products should be within two revision levels of the most current version supported by the software publisher and the Information Services Department. Servers with legacy operating system versions which have reached the software publisher's end-of-life should be at the last production release with plans to replace the operating system with a currently supported operating system as soon as possible. Special purpose servers not meeting these requirements must be registered in the County server database with additional information documenting the server function
2. System default administrator accounts password must be changed prior to placing the server on the production network. System default administrator accounts should be deactivated unless they are necessary for the proper functioning of server based software. Software that requires access to default administrator accounts should be avoided.
3. Any services or programs that launch automatically on boot-up which are not necessary for the proper functioning of a server must be disabled. Particular attention must be given to disabling SNMP if not used or changing SNMP community strings if it is used. Community strings must follow County password management standards.
4. Any services or programs that allow access and/or management of a server or its applications must not use system default passwords; anonymous accounts, default scripts or default access configuration strings.
5. The most recent security patches recommended by the Chief Information Officer must be installed on all servers connected to the County network as soon as practical. The Chief Information Officer must be notified if recommended

security patches are not installed within two weeks of the recommendation.

6. Trust relationships between systems are a potential security risk. Any trust relationships extending beyond organization boundaries must be reported and documented in the server database maintained by the Chief Information Officer.
7. Access to services should be logged and/or protected through encrypted access-control methods over secure channels, if possible. Remote administrator access must be performed over secure channels.
8. System Administrators should use the security principles of least required access to perform a function. Tree level access should not be used to perform branch level operations
9. Administrator and Root accounts should not be used when non-privileged accounts will do.
10. Servers should be physically located in an access-controlled environment and should not operate from uncontrolled cubicle areas.
11. All servers connected to the County network, whether owned by the County or other entity, must be continually executing approved virus-scanning software, with a current virus database, configured using settings published by the Chief Information Officer.
12. For disaster recovery purposes all production servers must be recoverable from backup copies no more than one business day old, through an off site backup method approved by the Chief Information Officer.
13. Automatic logoffs should be enabled at the network level and in sensitive applications where possible.
14. All server's and workstations must be set to limit the number of successive invalid attempts to logon. At minimum network user accounts should automatically lock following three invalid access attempts within any two-hour period of time. Accounts should remain locked for a minimum of two hours, unless reset by appropriate Information Technology staff.
15. Any deviations to these guidelines must be reported to the Chief Information Officer for inclusion in the server

database.

Workstations

As used here, "workstations" include desktop computers, portable computers and other general purpose computing devices used by end users to process computer instructions.

1. Desktop operating system versions for current products should be within two revision levels of the most current version supported by the software publisher and the Information Services Department. Operating systems for legacy devices should be at the last production release with plans to replace the operating system with a currently supported operating system as soon as possible.
2. Any services and programs that are not necessary for the proper functioning and intended purpose of a workstation must be disabled.
3. All workstations connected to the County network, whether owned by the County or other entity, must be continually executing approved virus-scanning software, with a current virus database, configured using setting published by the Chief Information Officer.
4. All workstations capable of time initiated security activity, such as password protected screen savers or automatic log off should have the security function enabled. Events should occur within fifteen minutes of inactivity on the workstation. Where possible and for Secure applications and systems, automatic logoffs should occur within ten minutes of inactivity.
5. User authorities, permissions and rights should be set at the minimum required to accomplish the user's job function. In Windows environments accounts with Administrator privileges should be reserved and restricted to functions and persons requiring those rights.

Departments must annually audit their workstations to determine manufacturer, model, workstation operating system version, operating system revision level, and virus scanning software and virus database version. Manufacturer's serial number and MAC address must be used to identify each workstation. A copy of the audit shall be provided to the Chief Information Officer for inclusion in a workstation database

Portable Computers and Portable Computing Devices

Portable computers and portable computing devices also known as Personal Data Assistants (PDAs) pose an increased security risk because they may contain private, confidential or sensitive County information, and being portable, are more at risk of loss, theft, or unauthorized access than standard desktop computers. As used here a PDA is any portable electronic device used to download information from, upload information to or otherwise communicate with the County network or any device attached to the County network. Examples of PDAs include Palm Pilots, Handspring Visors, Sony Clies, Microsoft products including Windows CEs, Pocket PCs, and Tablet PCs, Blackberry's and mini notebooks. In some cases these tools, both portable computers and PDAs, are the personal property of the employee rather than County but if they contain information obtained from the County network they are subject to County policies with respect to the acceptable use and security of that information.

No County employee may use a portable computer or PDA which is the personal property of the employee or some entity other than the County for County business purposes or a purpose that supports County business without the authorization of his or her department head or designee.

No County employee may download to, upload to, or maintain on a portable computer or PDA County information considered to be sensitive without the authorization of his or her department head or designee. County Information is defined as sensitive if it considered by the County to be confidential or may be damaging to the County, its employees, its customers or clients.

Employees assigned County-owned portable computers or PDAs are responsible for the security of the devices, all associated equipment and all data in the devices when they are taken to locations outside of County facilities.

Sensitive information that resides on portable computers and PDAs must be encrypted.

Departments are responsible for maintaining a current list of employees within their organizations who are using portable computers or PDAs that may be subject to this policy. This information is to be provided to the Chief Information Officer upon request for the purpose of trending the growth of these devices.

Wireless Systems

Access to the County network via unsecured wireless communication capable of transmitting packet data is prohibited. Wireless implementations must use encryption technologies approved by the Chief Information Officer. The Chief Information Officer must be informed of planned wireless implementations prior to their being brought on line and will maintain a database of approved wireless installations.

Modems and FAX Machines

Except for portable computers, where the intent of modem is for remote access into the County network, no modems may be attached to or installed in any computer connected to the County network unless approved by the Chief Information Officer. All modems must have the modem auto-answer feature disabled unless approved otherwise by the Chief Information Officer. Modems with auto-answer enabled must be set to answer no earlier than the fourth ring. Call forwarding services that permit forwarding calls to external telephone numbers must not be placed on any dial-up modem or fax telephone number within the County. The Chief Information Officer will maintain a database of approved modem installations.

Routers and Switches

This section describes a required minimal security configuration for all routers and manageable switches connecting to a production network or used in a production capacity at or on behalf of the County of San Mateo. All routers and switches connected to the County's production networks are affected. Routers and switches within internal, secured labs, not connected to the County backbone, are not affected.

The following configuration standards are required:

1. TACACS+ must be used for all user authentication's whenever possible.
2. Emergency local account passwords must be "single use" passwords.
3. All passwords on network devices must meet County password standards and be kept in a secure encrypted form.
4. The following must be disallowed:
   4.1 IP directed broadcasts
   4.2. Incoming packets at the router source with invalid addresses such as RFC1918 address
   4.3 TCP small services
   4.4 UDP small services
   4.5 All source routing
   4.6 All web services
5. Default SNMP community strings must be replaced with community strings published by the Chief Information Officer.
6. All console sessions must force a login.
7. Routers must be configured for auditing and every router command must be sent to an auditing server designated by the Chief Information Officer.
8. Access lists must be used to restrict the devices that can make requests or give instructions to routers and switches.
9. Router and Switches must have a designated point of contact and be included in a database maintained by the Chief Information Officer.

DMZ Servers

Devices that are Internet facing and outside the San Mateo County firewall, and devices that are inside the San Mateo County firewall which are exposed to the Internet by virtue of their relationship with Internet facing devices, are considered part of the "de-militarized zone" (DMZ) and are subject to this section. These devices are particularly vulnerable to attack from the Internet since they reside outside the County's firewalls. All server equipment or devices deployed in a DMZ owned or operated by San Mateo County or registered in any Domain Name System (DNS) domain owned by San Mateo County, must follow this policy unless a wavier is obtained from the Chief Information Officer.

1. All server configuration standards for internal servers are required configuration standards for servers in the DMZ unless otherwise approved by the Chief Information Officer.
2. Trust relationships between systems may only be introduced according to business requirements, must be documented, and must be approved by the Chief Information Officer.
3. Access control lists must be used to restrict services and applications not for general access.
4. Insecure services or protocols must be replaced with more secure equivalents whenever such exist.
5. Remote administration must be performed over secure channels or console access independent from the DMZ networks.
6. No data other than copied data may reside on servers outside the firewall.
7. All server content updates must occur over secure channels.
8. New installations and all configuration changes must follow the Information Services Department's Change Management process.

V. Application Development and Deployment

Departments should insure that any software purchased or developed for general use in the County has been tested and

properly operates on all hardware and software platforms for which the software is intended. Software that requires that the end user's computer workstation be configured with authorities beyond that of a common user should be avoided.
Application producers and developers must ensure their programs contain the following security precautions.

1. Applications should support authentication of individual users, not groups.
2. Whenever possible the use of system accounts rather than local user accounts should be used.
3. Applications should not store passwords in clear text or in any easily reversible form.
4. Applications should provide structured role management, so that administrative accounts can take over the functions of other accounts.
5. Secure systems should feature automatic user inactivity logoffs.

VI. Remote Access

This section defines standards for connecting to the County network from computers outside the County network. The standards are designed to minimize the potential exposure to San Mateo County from damage that may result from attachment to the County network, or from unauthorized use of County resources. The policy applies to all employees and other parties who connect to the County's network.
Authorized users and entities may access the County network only through systems and processes administered or approved by the Information Services Department. Users may access the County network via the Internet using a virtual private network client (VPN) approved by the Chief Information Officer or dial directly into a County-managed Access Server (modem pool).

1. Remote Access connections must adhere to the County's Acceptable Use and Password Management Policies.
2. It is the responsibility of individuals or organizations with Remote Access privileges to ensure that unauthorized users

are not allowed access to San Mateo County internal networks.

3. All computers connected to San Mateo County internal networks via a Remote Access technology must use an approved firewall and up-to-date anti-virus software, with a current virus database, configured using setting published by the Chief Information Officer. This includes personal computers and third party connections.
4. Remote connections will be automatically disconnected from San Mateo County's network after sixty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep connections open.
5. Only VPN clients approved by the Chief Information Officer may be used.
6. By using Remote Access technology with personal equipment, users understand and agree that their machines are a de facto extension of San Mateo County's network during connection periods, and as such are subject to the same security standards as apply to San Mateo County-owned equipment.
7. San Mateo County employees and contractors with remote access privileges must ensure that their remotely connected personal computer or workstation is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user. Vendors and other business affiliates who remotely connect to the County while connected a corporate network must be registered with the Chief Information Officer.

The Chief Information Officer must approve any exceptions to this policy. Exceptions will be maintained in an exception database and must be renewed annually.

VII. Employee Exit Procedures

Departments should establish Exit procedures so that when an employee leaves County Service and/or transfers to another department or division a structured exit process is followed. This process should include the recovery of all keys and badges and revocation of computer access, including the disabling of all network accounts, system accounts, application accounts, Email accounts and remote access accounts as well as revocation of voicemail account access. Departments should verify the integrity of systems and data turned over by departing employees prior to their departure.

Department System Administrators should audit user accounts on a regular basis. Accounts of employees who have left service should be disabled after a period of not more than five days. Employees who remain in service should not access accounts of employees who have left service except when directed by the department head. Accounts which have been inactive for more than thirty days should be disabled until a final disposition on the account has been determined.

VIII. Violations

Violations will be investigated and may result in disciplinary action up to and including dismissal from County employment, or cancellation of contractual relationship. For violations of patient confidentiality, the procedures of the Patient Confidentiality Sanctions Policy as regulated by HIPAA apply.