MARIPOSA COUNTY

Technical Services · (209) 966-8029

RESOLUTION - ACTION REQUESTED 2013-345

MEETING: August 13, 2013

TO: The Board of Supervisors

FROM: Rick Peresan, Technical Services Director

RE: Approve the Mariposa County Information Security Policy

RECOMMENDATION AND JUSTIFICATION:

Approve the Mariposa County Information Security Policy to enforce generally accepted best practice for information security and compliance with applicable federal and state law.

BACKGROUND AND HISTORY OF BOARD ACTIONS: The Board has approved information policies regarding email and general internet use in the past.

ALTERNATIVES AND CONSEQUENCES OF NEGATIVE ACTION: The County could be exposed to significant risk from information breaches and system outages.

ATTACHMENTS:
Mariposa County Information Security Policy (PDF)

CAO RECOMMENDATION
Requested Action Recommended

Rick Benson, County Administrative Officer 8/8/2013

RESULT: **ADOPTED [UNANIMOUS]**
MOVER: Kevin Cann, District IV Supervisor
SECONDER: John Carrier, District V Supervisor
AYES: Lee Stetson, Merlin Jones, Kevin Cann, John Carrier
EXCUSED: Janet Bibby

Mariposa County

Information Security Policy

Date: July 9, 2013

Mariposa County Information Security Policy

Table of Contents

Mariposa County Information Security Policy

I. Introduction

We live in a world where our information (data) resources are under threat from many areas. "Hackers" wander through public networks with general curiosity, "Crackers" search for the weak and unprotected organizations and attempt to damage information systems, demonstrating the ineffectiveness of your security initiatives.

Still, our biggest threat of intrusion to our Computer Information Systems can be traced to internal sources. Fully 70% of all attacks (denial of service, Trojan Horses, worms, viruses, etc.) are from internal sources. Visiting inappropriate website or downloading even seemingly innocuous toolbars and email stationary can introduce spy ware and viruses to our computer network. It is now estimated that 80% of all home PC's are infected with viruses and spy ware. Introducing data from home or non county computers infects our network causing outages and wasting hours of County staff time.

The existing threats and vulnerabilities to County information systems include, but are not limited to telecommunications, information systems, networks, and facilities.

The purpose of this document is to provide Mariposa County with an **Information Security Policy** that enables the County to administer "best practices" for information security and control. In addition this policy establishes guidelines for the proper handling and processing of computer generated functions relating to use of e-mail and Internet when accessed from County owned, leased, or controlled computers.

NOTE: This document does not address e-commerce authorities (i.e. electronic payments or acceptance of receipts), or web portal technologies. Any department that wishes to employ electronic receipts or payments must have a written policy approved by the Board of Supervisors.

II. Security Functions

A. System Owner

All access to system functions and data is determined by the application system or data owner. While the County is the "owner" of all information, the Departments are entrusted to authorize individual access to the systems. On their written authority only, the Technical Services Director will execute the necessary user ID access.

B. Security Officer

The Security Officer functions shall maintain records of all delegations, security profiles, and operator authorities. These shall be available for computer security audit and inspection. Each department must maintain records of user access to their application systems.

C. Change Control Coordinator

The Change Control coordinator function is responsible for establishing, maintaining, and monitoring intrusion detection and use of the security features of the computer systems. The Change Control Officer may also review Internet and E-mail usage during analysis of the activity log files in the network firewall, content filtering software, or E-mail server in search of intrusion or inappropriate Internet access. This task is the responsibility of the Technical Services Director.

NOTE: Under no circumstances will the Security Officer, Change Control Coordinator or any system administrator access individual data files without the written permission of the file or system owner with the exception of a written request from County Counsel or the County Administrative Officer.

III. System Access Controls

A. Network Access

The means of securing access to the network, programs, and data files will vary from one type of machine or connection to another. The objective is to create an environment in which the integrity of programs and data can be established and maintained, such that the County is not exposed to risk of loss arising from fraud or disruption of data processing. It is the policy that, unless otherwise approved, access to the network is restricted to county owned computers. Any non County administered computer must certify the device is protected with current antivirus software (see appendix B form).

1. Prior to installation, all network access points shall be reviewed by the Department head to determine intrusion risk and are encouraged to contact the Technical Services Director for advice on appropriate action.

These include:

   a. Dial up network connections to the Mariposa County Network or the Internet.
   b. Wireless network connections to the Mariposa County Network or the Internet.
   c. Public switched telephone network connections (PSTN) to the Mariposa County Network or the Internet.
   d. Digital Subscriber Link (DSL) connections to the Mariposa County Network or the Internet.
   e. Virtual Private Networks (VPN) to the Mariposa County Network.

2. Network design shall treat all transactions outside of the LAN as non-trusted transactions, secured via authentication devices or firewalls.

3. Dial up modem connections shall be eliminated wherever feasible because they are particularly vulnerable to foreign intrusion.

4. File sharing configurations and PC application systems shall be eliminated in favor of network server file storage.

5. Network access controls shall be installed on all networked computer systems to prevent the deliberate or accidental unauthorized access that could result in the perpetration of fraud or the corruption of data.

6. Public access computers shall have limited inquiry only access to public data.

7. Hardware and software manufacturer default user ID's and passwords shall be changed immediately on installation of the products. In the case of external vendor access for maintenance and support, login profiles shall be deactivated

until the vendor requests access or otherwise approved by the Department Head or Technical Services Director to assure business continuity.

8. Any data transfer from an outside source (floppy, CD or memory stick) must be reviewed by the Technical Services Director, Department Head or designee to avoid virus or spy ware infection from an outside source. No employee can use a floppy, CD or memory stick on any county owned computer without prior approval.

9. Any non-County owned computer that needs connection to the County network must be reviewed for valid antivirus and licensed software.

10. Any program loaded must be reviewed by the Technical Services Director, Department Head or designee to avoid negative impact to the device or network.

B. Passwords

It is essential to resist the temptation of taking the view that colleagues are known, trusted, and that their time is valuable, so that it is not justified to slow down their work or restrict their access. Generally accepted best practices demands segregation of duties and it is irresponsible to place colleagues in a position of suspicion by failing to establish proper security controls.

1. Different computer operating systems provide some, all or variations of these controls. Where possible, users shall be able to change their own passwords. It is strongly recommended that passwords contain a minimum of eight characters and use numbers and special characters.

2. Passwords are the key to accessing computer systems and so it is important that they are properly controlled. Each user is identified to the computer by means of a password, and shall be held accountable for any activity on the computer using their ID.

3. Whenever possible, at least two barriers shall be placed in the way of unauthorized access such that shall the first barrier be accidentally or deliberately breached, a second barrier will assuredly prevent the access which should not be allowed. This would include using a separate PC logon password and a separate application password.

4. Screen saver passwords shall be employed wherever possible. Using a screen saver password, set to trigger when inactivity is detected on the device, prevents unauthorized access when the computer is unattended.

5. An annual review, re-validation, and audit of system access controls shall be conducted annually by the Security Officer.

6. Technical Services Department staff will assign each user a password when the related user profile is created on the computer system.

7. Where the system permits, the Change Control Coordinator will "pre-expire" the initial password, thus forcing the user to change it and assume accountability when first accessing the computer.

8. Computer users shall keep their passwords secure at all times, shall not record them in a recognizable format, and shall not divulge them to any other person. If a user suspects that their password may have been compromised, they shall inform their supervisor immediately and change their password.

9. Where a system does not provide automatic control, such as requiring a digit in the password, users should follow these guidelines:

    a. The password should be changed at least every 180 days.
    b. The password should be a minimum of 8 characters long.
    c. The password should include at least one digit, punctuation mark or special character.
    d. The password should not contain more than two successive repeats of a character or digit.
    e. The password should be different from at least the last six choices.
    f. The password should not be obvious such as a word, variation on a name or the same as the user ID.
    g. The password should not follow a simple sequence such as 123456 or ABCDE.
    h. Under no circumstances should users share passwords.
    i. "Remember" password functions should not be enabled for any programs or Internet applications.

C. Encryption

1. It is the responsibility of each Department to assure encryption of personal identification, sensitive, health, or confidential data transmitted from County computers through the Internet. Questions on encryption should be directed to the Department Head or Technical Services.

D. Web Pages

1. It is County policy that all County departments shall establish their web pages and E-mail addresses under the County's official domain only, as designated by the Technical Services Department under direction of the Board of Supervisors.

E. Internet Browser

1. It is recommended that all internet users employ the Microsoft Internet Explorer for use as the Internet browser. In addition, no settings may be changed by the

individual user without prior consent from the Mariposa County Technical Services Department.

F. E-mail Client

1. The County policy is that all county E-mail users must employ the Mariposa County e-mail system and use the Microsoft Outlook E-mail client. No other E-mail client or E-mail system may be installed without the approval of the Mariposa County Board of Supervisors.

G. Email Retention

1. E-mail is retained electronically for a period of 180 days. However, it is County policy that all departments adhere to their legal record retention requirements. Email should be printed and filed in the appropriate location if any law or department policy expressly requires communication retention for a period greater than 180 days.

H. Anti Virus Software

1. Antivirus software must be installed and remain active on each County computer. The user must notify the Technical Services Department if the anti virus software is not active on their PC.

I. Responsibilities

1. It is each Department Head's responsibility to ensure appropriate use of e-mail and Internet resources within its department and that it is consistent with the County's Policy at large.

2. It is each Department Head's responsibility to ensure compliance with California Senate Bill 1386 (SB 1386), which mandates that companies disclose publicly when customer information stored on their networks has been accessed in any unauthorized manner.

3. Department Heads and supervisory personnel are responsible for ensuring that all users of e-mail and other Internet access programs receive a copy of this Policy and that such receipt is documented.

4. Any County pertinent data must be saved / stored on the local area network. No personal information should be stored on the network.

IV. Internet Access and Electronic Mail Policy

The purpose of this policy is to establish guidelines for the proper handling and processing of computer generated functions relating to the use of e-mail and Internet when accessed from County owned, leased or controlled computers.

The Board of Supervisors recognizes the right of every Department Head to determine the need for Internet access and the use of e-mail to assist them in the execution of County business.

A. Definitions

1. E-MAIL: E-Mail shall mean any computerized system or software designed for the transmittal of written messages either with or without attachments, from one person to another, from one computer to another, or from one or more e-mail addresses to one or more other e-mail addresses. E-mail shall include such messages generated from personal, network, desktop and/or laptop/notebook computers, as well as mobile digital terminals or vehicle-mounted systems.

2. INTERNET: Internet shall mean any computerized information source accessed via modem or other means from a source external to or apart from the computer or computer network through which the information is sought.

3. DOWN LOAD: The transfer of files or e-mail from a source external to the local personal computer or local area network.

B. Disclaimer

Mariposa County is not responsible for material viewed or downloaded by users from the Internet. The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. In addition, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Users accessing the Internet do so at their own risk.

C. Policy

1. Employee's duty of care: Employees should use the same care in drafting e-mail and other electronic documents as they would for any other written communication. Please keep in mind that anything created or stored on the computer system may, and likely will, be reviewed by others. Individual users must be aware of, and at all times attempt to prevent, potential County liability in their use of the Internet.

2. Unless authorized in accordance with Section IV. C4., e-mail systems are to be used only for County business-related purposes; and all messages sent, received, or stored are treated as business messages. Unless authorized in accordance with Section IV. C4, employees shall not access the Internet while on duty except for purposes directly related to work being performed in furtherance of County business. The County reserves the right to monitor, access, copy, delete, and use for County purposes, any messages being received, received, or stored on County-owned computer systems. No individual should have any expectation of privacy for messages or the data recorded in, sent through, or received via a county agency terminal.

3. While County electronic e-mail retention is for a period of 180 days, an e-mail communication should be deleted as soon as practicable from the system. It is the policy of the County of Mariposa that e-mail is not to be used to retain or store public records of any department or agency of the County. Communications or records intended or required by law to be retained shall be printed in a hard copy and filed or stored as appropriate or saved to designated electronic files or other media as required by departmental or agency procedures. It is County policy that all departments adhere to their legal record retention requirements. E-mail should be printed and filed in the appropriate location if any law which expressly requires a communication to be kept for a period greater than 180 days. Employees should seek guidance from their Department Heads in order to ascertain the specific time requirements applicable to the documents generated, received and or maintained by their department.

4. Personal e-mail communications and Internet access. An employee's Department Head or their designee may permit personal e-mail communications as well as personal access to the Internet. If personal use is permitted, the Department Head shall establish procedures to assure use is not abused. Employees should carefully note, however, that only their Department Head or their designee, determine what is or is not "authorized use." Further, by use of a County system for e-mail and Internet access, employees consent to monitoring of messages or on-line activity, regardless of whether the use is authorized or unauthorized, official or personal. The fact that an employee may consider a message to be personal does not mean that it is private--it isn't. As such, e-mail may be reviewed by the employer in the ordinary course of business, without notice to the employee. Personal usage is also subject to the following limitations:

    a. Use does not adversely affect the employee's performance of duties.

    b. Use is of reasonable duration and frequency and, is made during the member's personal time, i.e., breaks and lunch.

    c. Use serves a legitimate public interest, such as keeping employees at their workstations, improving morale, enhancing professional skills, or furthering education.

d. Use does not adversely reflect on the County of Mariposa by any use that is incompatible with public service including, but not limited to, uses involving pornography, chain letters, advertising, or soliciting, or any use that could reasonably be conceived as creating a hostile work environment, or harassment, etc.

e. Use does not create additional costs to the County of Mariposa.

5. County e-mail may be subject to public disclosure. Messages shall be professional and courteous.

D. General Guidelines

1. Confidential County information shall be transmitted only to those authorized to receive it. Additionally, when such confidential or restricted information is transmitted over the Internet, it must be sent in an encrypted form. Exceptional care is to be taken to insure confidential materials are not mistakenly transmitted to unauthorized recipients.

2. Copyrighted Information - Use of County e-mail to copy and/or transmit copyrighted documents, software, or other information must comply with the laws permitting such use of copyrighted information.

E. Other Prohibited Uses

1. E-mail/Internet access shall not be used:

a. In violation of any law or County policy.

b. To transmit defamatory, obscene, offensive or harassing messages, or those conveying threats, slurs, or other inappropriate messages.

c. To transmit messages disclosing personal information without authorization.

d. To transmit private mass mailings.

e. To run or otherwise manage a personal business using a County computer.

f. To view, forward or otherwise publish sexual or obscene material.

g. To publish Web "Blogs" using County Equipment or Internet Access Infrastructure.

h. To play games of any kind.

i. To listen to music.

j. To allow a non-County employee to use computer equipment without authorization from their Department Head.

2. Downloading files and/or programs (note: this prohibition does not apply to e-mail) from the Internet or loading any software programs without the Department Head's approval or any other misuse are prohibited actions and employees can be disciplined for violating these rules. Employees shall immediately advise their supervisor in writing of any data or material downloaded to the employee's e-mail address and/or computer terminal, involving pornography, inappropriate solicitation, or material that could reasonably be conceived as creating a hostile work environment or harassment. Failure to so advise one's immediate supervisor will result in a presumption that the employee intentionally downloaded and/or retained the material in question.

   If files, for whatever reason, are introduced to a County computer via external media, the file(s) must be scanned by approved antivirus software before moving to a County computer by a supervisor or manager.

3. Employees are reminded that log-on and other passwords are confidential and must be properly safeguarded. We require passwords to protect information from improper review by other employees or individuals, outside of Mariposa County. Passwords are not intended to shield e-mail/internet records from appropriate review by authorized Mariposa County employees.

F. Violations

1. Violations will be investigated and may result in disciplinary action.

G. Summary

In summary, all employees must recognize that e-mail and Internet access is used for official and authorized purposes only, unless otherwise approved pursuant to Section IV, C4. In addition, employees should apply the traditional notions of good judgment, common sense, and professionalism. Finally, when in doubt, employees should seek guidance from their Department Head.

H. Social Awareness

Our society and culture promotes a friendly and helpful human nature. We are a very trusting society. When people attempt to gain access to an area or request information, our first reaction is to help. Either by opening doors, answering questions or directing them to private locations. Unfortunately, this kindly attitude can lead to serious security and safety concerns. It is not uncommon for people to try and gain access to locations they do not and should not have access, only to find a helping hand to open doors or reveal information that can be used to perpetrate fraud or endanger employees.

1. While it is not the intent to create a hostile environment, County employees shall maintain awareness of a potential security or safety problem. Never confront a stranger in a threatening manner, but do not hesitate to ask what business they may have and how you may help them.

2. Do not offer non-public information. If questions persist, ask the individual to wait for a manager or Department Head. If they are in a restricted area ask them to leave or escort them to an appropriate waiting area.

3. If you suspect trouble, contact the Sheriff's Office immediately. You should report any suspicious activity or incidents to a manager, Department Head, or Sheriff's Deputy.

4. It is the responsibility of every employee to report deficiencies in security to the Security Officer or Department Head.

V. Business Continuity

A. Data Backup

1. Production data backups, regardless of computing platform, shall be on a schedule related to the rate of change and level of risk should an outage occur. Backup media shall be stored on site (same location as the computer) and off site (alternative storage in case of damage to the central facility) on an alternating basis.

2. Minimum standards for networked system data (AS400 and network server) backups:

   a. Daily backups for all data files that have changed that day.
   b. Weekly backups of all data regardless of the last changed date.
   c. Monthly backups of all system data and programs.
   d. Full system backups prior to any system upgrade.
   e. Full system backups after any system upgrade.

3. Minimum standards for PC data:

   a. Daily backups for all data from an electronic source (not manually entered).
   b. Weekly backups for all data that changed from the last backup.
   c. Monthly full system backups.
   d. Full system backups prior to any system upgrade.
   e. Full system backups after any system upgrade.

4. Backup copies, both onsite and offsite shall be stored in an environmentally stable, fire proof and secure location offsite that permits access in case of emergency.

B. Disaster Recovery

1. The Technical Services Director shall create an Information Systems Disaster Recovery contingency plan document, approved by the System Owner (Department Head) and Board of Supervisors, to:

   a. Verify responsibility for implementation of the plan.
   b. Individual assignment of staff responsibilities.
   c. Defend priorities for various types of failure.
   d. Locate names, addresses and telephone numbers of responsible individuals.
   e. Identify location of all backup media and equipment.
   f. Fall back procedures which include manual procedures to follow during periods of computer failures.

2. Each application system shall be evaluated for the impact on County Business for different types and severity of failures.

    a. Determine the maximum time available before each type and severity of failure has significant adverse effect on business (may vary by time of month or year).
    b. For hardware, arrange the agreed contingency.

VI. Physical Controls

A. Locations

1. It is the responsibility of the Technical Services Director to assure all locations of network computer equipment shall:

    a. Be in a secure location, where access to the equipment can be limited to authorized personnel.
    b. Ensure adequate, clean power supply.
    c. Provide central power on off switches (separate breakers).
    d. Employ back up power supplies (UPS).
    e. Provide sufficient space for computing equipment.
    f. Provide and maintain sufficient heating and air conditioning dedicated to the computer area.
    g. Provide wire management systems to ensure safe, stable environment
    h. Ensure area is cleaned regularly.
    i. Prohibit eating, drinking, and smoking.
    j. Provide Halon (or substitute gas) extinguishers for electrical fires and verify they are regularly tested and inspected.
    k. Provide large plastic sheets to cover equipment in case of water leakage.

B. Computer Output

1. Ensure that formal procedures exist to ensure that production reports, microfilm, and other output, is only distributed to authorized staff.

C. Laptop Computers and Mobile Phones

1. It is the responsibility of the user to maintain physical security of the computer to protect against theft or loss.

2. Wireless network adapters should be disabled when not in use to protect against outside intrusion of County data.

3. It is the responsibility of the user to report lost or stolen equipment to the Department Head and the Technical Services Department. If it is a personal device with County data, contact your carrier to disable and inform your Department Head.

4. For personal devices, the user must obtain prior approval from their Department Head before using the device to store and transmit County data.

VII. Data Ownership

1. Each application system shall have an assigned application owner. The application owner is a Department Head or their designee, empowered to approve access to the system data.

    a. User access to an application system shall be approved by individual's manager and the application owner.

VIII. Virus Detection Software

1. All networked Personal Computers and Servers shall have virus detection and prevention software running on startup of the equipment. The virus detection software shall be approved by the Technical Services Director and shall be configured to delete suspected files without user option.

Appendix A.

A. Information Security Policy Agreement Form

Mariposa County
Information Security Policy
Agreement Form

The County reserves the right to monitor and log all network activity including e-mail and Internet use, on County owned computers, with or without notice, and as a user; I understand that I have no privacy in the use of these resources. Internet activity may be reviewed and may be analyzed for usage patterns, and reports may be publicized.

The County may have software and systems in place that can monitor and record all Internet usage. I am aware that security systems are capable of recording (for each and every user) each World Wide Web site visit, each chat, news group or electronic mail message, and each file transfer into and out of our internal networks, and the County reserves the right to do so at any time.

I agree that all computing activity conducted while performing County business and/or conducted with County resources is the property of Mariposa County. In addition to the terms specified herein, I have received a copy of the "Mariposa County Information Security Policy", have read and understand their requirements and information, and agree to abide by and conduct my use of the Internet in accordance therewith.

Signed: _____ Date: _____

Printed: _____

Department Head: _____ Date: _____

Copy to be filed with Mariposa County Human Resources

Appendix

B. Device Certification Form

Mariposa County
Device Certification Agreement Form

I certify the device I connect to the Mariposa County computer network is professionally administered, contains legally licensed copies of software and has a current antivirus subscription and data file.

Signed: _____ Date: _____

Printed: _____

Department Head: _____ Date: _____

Copy to be filed with Mariposa County Technical Services