INFORMATION TECHNOLOGY POLICY BOARD

ADOPTED STANDARDS/POLICIES

Information Technology Security Policy

COUNTY OF SACRAMENTO

Office of Communications and Information Technology

PATRICK L. GROFF
Chief Information Officer

April 25, 2000

TO:
Agency Administrators, Department Directors

FROM:
Patrick Groff
Chief Information Officer

SUBJECT:
COUNTY OF SACRAMENTO INFORMATION TECHNOLOGY SECURITY POLICY

The County's Information Technology Policy Board (ITPB) has approved the attached Information Technology Security Policy. We hope that this revised Policy will help all of us by providing a consistent framework for safeguarding our County's IT resources, equipment and information.

This Policy is designed to be general in nature and you may find that the needs of your departments may be greater than what is provided in the Security Policy. You are encouraged to create a companion policy to meet the unique situation in your department.

Please note that the new Policy requires that all users sign an Acknowledgement of Information Security Responsibility. (*See paragraph 6*) Each department should maintain signed copies of this acknowledgement document in their personnel files.

We have developed this Policy to clarify the appropriate use and ownership of the County's IT resources, data and equipment. It is important to recognize that the overwhelming majority of County employees are conscientiously using County IT resources in an appropriate manner. However, there have been a few situations where departments have had to deal with inappropriate use, especially in the areas of e-mail and internet access. This revised Policy addresses unacceptable use and content. (S*ee paragraph 3*)
If you have any questions contact me at 874-7825.

Concurrence: _____
Terry Schutten,
County Executive

COUNTY OF SACRAMENTO
INFORMATION TECHNOLOGY SECURITY POLICY

Preface

Purpose

This document states the information technology (IT) security policies for the County of Sacramento. It applies to all County employees, both permanent and temporary, and all contractors, consultants, vendors, interns, volunteers and others who use County-owned or leased IT resources. This document does not supersede federal, state, or local regulations governing the use of information technology.

For the purposes of this document, the term user refers to any employee (permanent or temporary), contractor, consultant, vendor, volunteer, student or other person who uses, maintains, manages or is otherwise given access privileges to County IT systems. Additionally, the phrases "IT system" and "IT resource" include all computer, telephone, and radio hardware (including peripherals), software applications and data (including electronic and voice mail), networks and network connections (including to the Internet), documentation and other capabilities intended for the purpose of processing, transferring, or storing data in support of County goals.

Comments and suggestions affecting this document should be forwarded to the Chief Information Officer (CIO) for review and incorporation. Before being implemented, changes to this document will be reviewed by the Technology Review Group (TRG) and must have the approval of both the CIO and the Information Technology Policy Board (ITPB). At least annually, the ITPB should review this document to determine whether additional changes are required.

Background

The IT needs of the County of Sacramento have changed dramatically over the past years. The information requirements of County customers and employees have increased and the technology required to process that information has diversified. County information is now distributed across many systems consisting of various combinations of hardware and software. Because information can appear in many formats and on different systems, the potential for misuse or loss is very high. While IT offers improved communication and information sharing, it brings with it increased vulnerability. Since County IT users are increasingly dependent on accurate and reliable information systems, it's important to protect County IT systems from misuse.

Conclusion

This policy states each individual's responsibilities for maintaining the security of County IT resources. It will help coordinate inter-department security efforts and improve the County's overall security posture. Department Heads and Agency Administrators should supplement this policy with a department or agency policy that addresses specific, department or agency-unique security requirements.

Respectfully Submitted,

LEE ISMAIL, Chair	PATRICK GROFF
Information Technology Policy Board	Chief Information Officer

Policy

1. IT Resources

All County IT resources shall remain the property of the County of Sacramento and may be examined at any time. Users must not install, upgrade, repair or move IT resources without IT management approval. Proprietary or County-developed software must not be copied or distributed without management approval.

Only County-approved equipment is to have a permanent physical connection to County networks. Users should consult with their System Administrator for the proper use of portable devices and the relocation and reconnection of desktop devices.

The County cannot support unapproved IT resources. Installation, upgrade, repair or other forms of support will only be performed on official County-owned, leased, or licensed IT resources.

2. User IDs and Passwords

No user will give his or her password to another person unless that person is authorized to receive such information. If a password is compromised for any reason, the password shall be changed as soon as practical. Users shall choose passwords in accordance with the “Password Construction Guidelines” in Appendix 1 of this policy.

3. Unacceptable Use and Content

Users must not use County IT resources for purposes other than those that support official County business or as defined in this policy. Users must not use County IT resources for commercial financial gain or to conduct illegal activities. Personal use of County IT systems can be approved by Department Heads and Agency Administrators. Specific restrictions should be defined in department or agency supplements to this policy

Except for authorized criminal investigations, users shall not use County IT resources to access offensive material on Internet sites, call telephone services, or otherwise send or receive offensive material. Offensive material includes, but is not limited to, sexual comments or images, racial slurs, gender offensive comments, or any comments that would be offensive on the basis of age, sexual orientation, religious beliefs, national origin, or disability.

"Users must not send sensitive information via the Internet unless a County-approved form of encryption is used, the information is transmitted via sites that support industry adopted security standards, the transfer is authorized by Department Head or Agency Administrator, or where required by law."

4. Voice/Electronic Mail

All voice-mail and e-mail messages composed, sent or received using County IT resources remain the property of the County at all times. The County reserves the right to retrieve and read any message composed, sent, or received using County IT systems. Voice mail and e-mail will not be distributed to users other than the intended recipient except at the direction of the recipient, a Department Head or Agency Administrator.

Within a voice-mail system, users may be required to share a password among two or more individuals. If the business environment requires shared voice-mail accounts, the Department Head or Agency Administrator will define procedures explaining how the accounts will be managed.

Users should report to their supervisor if they receive voice-mail or e-mail containing content that may be reasonably considered offensive or disruptive. Supervisors, managers and system administrators who investigate reports of unsolicited material must not compromise the confidentiality of the individuals involved.

5. Workplace Privacy

System administrators are authorized to examine and/or retain files within the scope of their responsibilities to troubleshoot and/or repair the IT resources under their purview. System administrators must not disclose the contents of such files unless the contents are in violation of this policy, other County, department or agency policies, or federal, state, or local law. Content in violation of policies or the law will be reported to management.

The County may inspect, review or retain any personal electronic mail or any other personal computer records generated by any user of County IT resources. A user shall be permitted, subject to the limitations contained in Government Code section 31011, to review any data pertaining to the user that is collected by the County in the course of monitoring electronic records and communications and to dispute and have inaccurate data corrected or deleted.

6. Acknowledgement of Information Security Responsibility

All users must sign an Acknowledgement of Information Security Responsibility.

Appendix 1 – Password Construction Guidelines

Select Good Passwords

Good passwords should be easy to remember, but hard to detect. Intruders use many tools to try to extract passwords from system password files. Here are some helpful tips to construct passwords that would be difficult to detect.

- USE at least six (6) characters. Passwords of less than 8 characters in length should be randomized (e.g. "PojGoar") or incorporate numbers (e.g. "go3267").
- USE a long word and truncate it to eight letters, but don't use "sacramen".
- USE an 8-letter phrase that is not easy for computer hackers to guess (e.g. "reallife").
- USE a combination of 7 letters and a number, 6 letters and 2 numbers, etc. (e.g. faren451"), but don't use sequential numbers (e.g. "12345678") or dates (e.g. july1998).
- USE a special character such as ~, !, @, #, $, %, ^, &, *, (,), in between words, but check with your system administrator before you do. Some computers don't accept special characters.
- USE two words (e.g. pit-stop) or misspelled words (e.g. "pyt-stop").

NOTE: Many computers cannot accept spaces as valid password characters. If you use a space, the system may only accept and recognize the first few characters; truncating the rest of your password. Also, be aware of systems that are case-sensitive.

If you're not sure whether your selection is good, check it with a dictionary. If you find your password in a dictionary, then it's a bad password.

Practices to Avoid

Good passwords should be easy to remember, but hard to guess. Intruders use many techniques to try to guess passwords. Here are some tips to avoid passwords that would be easy to guess.

- DON'T use nothing at all. Blank passwords are usually an intruder's first guess.
- DON'T use your User ID. User IDs are widely distributed through e-mail and phone lists.
- DON'T use words such as "password", "secure", "secret", "confidential", "restricted", or "private".
- DON'T use words such as "computer", "network", "workstation", "server", "router", "windows", "unix", "dos", "microsoft" or anything to do with computers.
- DON'T use your name, your nickname (or any other alias), your spouse's name, your children's names, or (my favorite) mother's maiden name.
- DON'T use the words "mother", "father", "sister", "brother", or any other genealogy term unless personalized. For example, the term "uncle" is bad, "unclejon" is better, and "unclej0n" (where "0" is a zero) is best.
- DON'T use "sex", any variant of "sex", anything to do with "sex", or any obscene word for that matter.
- DON'T use obvious words and phrases like "start", "start-it", "start-up", "open", "open-up", "opensesame", "opensezme", "its-me", "let-me-in", "access", "access-it".
- DON'T use obvious, job-related terms such as "sacramento", "county", "california", "ocit-cio", "audit", or "sheriff" particularly if they're related to YOUR job.
- DON'T use cyclical passwords such as the name of the current month. Cyclical passwords are easy to guess.
- Avoid names or words associated with your hobbies, favorite books or movies, car or driver license number.
- And be careful using foreign languages – they may fool Americans, but they won't fool foreigners. DON'T use the words shahnghwa (Chinese), contraseña (Spanish), clave (Spanish), kennwort (German), erkennungswort (German), Paßwort (German), aikotoba (Japanese), or pasuwaado (Japanese). All of these words translate to the English word "password". Since the Internet is global, intruders could attempt to break-in from any country in the world.

And, avoid using script files, macros and options with embedded passwords to automate your login process.

Use Different Passwords on Different Systems

Passwords used for secure access should be different than those used for non-secure access. Use different passwords to separate public, private, and personal information. For example, use one password to access non-sensitive County data (e.g. your LAN account), a second password to access sensitive data (e.g. your mainframe or enterprise server account), and a third to access public systems (e.g. your Internet Service Provider). Although user IDs should be the same for a single user across many systems, don't use the same password across all systems.

Appendix 2 – Glossary of Terms and Definitions

Terms

CIO	Chief Information Officer
ID	identification [code]
IT	information technology
ITPB	Information Technology Policy Board
LAN	local area network
TRG	Technology Review Group

Definitions

IT Manager	IT managers supervise, direct, or otherwise manage system administrators and the IT systems that they administrate.
IT resource	The phrases "IT system" and "IT resource" include all computer, telephone, and radio hardware (including peripherals), software applications and data (including electronic and voice mail), networks and network connections (including to the Internet), documentation and other capabilities intended for the purpose of processing, transferring, or storing data in support of County goals.
IT system	See "IT Resource".
password	A sequence of characters which verifies the user's identity.
permanent physical connection	A permanent physical connection is defined as an IT resource which is located in or on County property that has a dedicated wire (or wireless) channel which provides access to County-owned IT resources and does not require a login sequence in order for other computers on the County network to be able to connect to that IT resource.
sensitive information	Sensitive information includes both "sensitive data" and "confidential data" as defined in the Electronic Data Access Policy (Electronic Access to Public Information) for the County of Sacramento (February 24, 1999), and other data as defined in department and/or agency policies.
software	The term software includes applications, data files, documents, databases, other information or information systems
system administrator	A system administrator is an individual assigned to configure, maintain, or monitor the performance of one or more County IT resources. The phrase also refers to network administrators, LAN administrators, logon administrators, security administrators, system supervisors, or any other such job title where the individual can access and modify the technical configuration of the computer.
temporary physical connection	A temporary physical connection is defined as an IT resource which must go through a login sequence in order for other computers on the County network to be able to connect to that IT resource.
user	For the purposes of this document, the term user refers to any employee (permanent or temporary), contractor, consultant, vendor, volunteer, student or other person who uses, maintains, manages or is otherwise given access privileges to County IT systems.
user ID	An identification code which identifies the user to County IT systems

COUNTY OF SACRAMENTO

ACKNOWLEDGMENT OF INFORMATION SECURITY RESPONSIBILITY

I, _____, recognize and understand that the purpose of the County's information technology network, including its computers, telephones, radios and other resources is to support County business. I agree not to use any application, access any file or retrieve any stored communication other than where authorized unless there has been prior clearance by an authorized representative.

I am aware that the County reserves the right to audit, access, and review all matters on the County's information technology network, including e-mail and voice mail messages at any time, with or without notice, and that such access may occur during or after working hours. I am aware that use of a County-provided password or code does not restrict the County's right to access electronic communications and that, except where prohibited by law, the County will disclose any and all information required by the law.

I am aware that if I violate this policy, I may lose any access privileges granted by the County and be subject to disciplinary action up to and including termination or, if I am not a County employee, termination of my contract.

I acknowledge that I have read and I understand the County's Information Technology Security Policy.

_____ _____

Signature Date Signed