COUNTY OF TUOLUMNE

Information Technology (IT) Policy

Prepared by:
County Administration Office
Information Systems and Services Division

November 20th, 2001

County of Tuolumne

Information Technology (IT) Policy

November 20th, 2001

Table of Contents

1. Introduction

1.1 Background

The Information Technology (IT) needs of the County of Tuolumne 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 the new format of IT offers improved communication and information sharing, it brings with it increased vulnerability. Since County IT users depend on accurate and reliable information, it is important to properly manage County IT systems.

1.2 Purpose

This document states the IT security policies for the County of Tuolumne. The policies in this document apply to all County employees, both permanent and temporary, and to all contractors, vendors, interns, elected officials, volunteers, and others who use County-owned or leased IT resources. This document does not supercede 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, elected official, 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 hardware (including peripherals), radio hardware, software applications and data, 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.

This umbrella policy sets forth rules on the management and use of County IT facilities, systems, and resources using the principle of Custodianship. Custodial Agencies and Department Heads are directed to develop internal supplemental policies as required. It is the individual user's responsibility, as well as his or her Custodial Agency's responsibility, to uphold the policies set forth in this document and the policies required by this document. A violation of the policies in this document or of the policies authorized or required by this policy (subject to collective bargaining) may result in disciplinary action up to and including termination. The word "policies" includes standards, procedures and rules.

Comments and suggestions affecting this document should be forwarded to the County Administrator for review and incorporation. Before being implemented, changes to this document will be reviewed by the IT Security Policy Committee (ITSPC). The final interpretation of the changes will be by the County Administrator, which then will be

approved and adopted by Board of Supervisors. At least annually, the ITSPC should review this document to determine whether additional changes are required

1.3 Principle of Custodianship

The concept of the Custodianship, rather than the ownership of data, is one that has always been implicit in the management of public information. However, prior to the widespread use of computer networks, it was a concept that could be honored in theory while being ignored in fact. Computer networking has very much changed this. Heretofore, information, though public by law, was difficult to search out because it resided on paper within tons of other documents in the county archives. Even with the introduction of computers, the information that was entered into the electronic medium was on stand-alone devices, allowing each department to have a feeling of ownership rather than custodianship due to the insularity of the data. It was only with the linking of computers over networks that this attitude about public data has had to change. Despite the fact that there is no way of knowing what the value of information collected by one department might be to another department, the sharing of this information must always be advantageous. The legitimate use, that is a use driven by some concern for the good of the populace of the County, by other County Departments of the data that has been collected by one County entity, must be viewed in the most positive of manners by the departments concerned.

Custodianship encompasses more than just sharing of data. It implies that the County entity that collects this data is charged with ensuring that the collected data is as accurate as possible and guarded in accordance with the rules of privacy prescribed by law, that data does not become lost, and that an atmosphere is engendered such that the sharing of data is made as easy as possible not only physically, within the bounds of the equipment on which it is stored, but also with a willingness on the part of the staff to provide the data to others, that it may ultimately benefit the citizens of the County.

1.3.1 Identification of the Custodians

Identification of the custodians must be explicit, but is increasingly complicated as offices share information and computerized databases. Resolving custody identification issues may impact current organizational forms. The Board of Supervisors shall, by resolution, adopt a list of County Custodial Agencies and their specific duties.

1.3.2 Definition of Custodianship

Custodianship encompasses the collection, storage, safeguarding of the data's logical integrity, dissemination, ordering, setting of standards for, insurance of integrity of, awareness of impact on other agencies by, and quality assurance of data that is the property of the County of Tuolumne. Custodians are the trustees and not the owners of the data or the system on which it resides. Refer to *Appendix 1* for specific duties of the Custodian.

1.4 Custodial Agency Policies

This policy document requires that each Custodial Agency develop supplemental policies to address the needs and the use of the data and information under their custodianship. Such individual policies may not violate any rules set forth in this policy, unless it is demonstrated that a particular Custodial IT system or resource has a limitation or requirement which this document overlooks. With this respect, Custodial Agencies shall document the statutory requirements and limitations associated with the data and information in their custody. Every policy defined by Custodial Agencies must be submitted to the County Administrator for review and approval. In the case of conflict, resulting from an overlapping of jurisdiction or from challenges to the approval or disapproval of access right, between two or more Custodial Agencies or between Database Administrator (DBA) and Custodial Agency, the conflicting parties will appeal to the County Administrator for the arbitration of conflict. Further – all custodial agency policies will be reviewed and approved as to legal form and content by County Counsel. The requirements, which Custodial Agencies must comply with in order to fulfill the obligations set forth in this document, are listed in *Appendix 2* of this document.

1.5 Final Interpretation

Notwithstanding any other provision contained in this document, the County Administrator will resolve any conflicts regarding the interpretation or implementation of this policy.

2. Definitions

Refer to *Appendix 3* of this document for a list of technical terms and their definitions.

3. Policy of Access

3.1 Physical Access

Physical security of IT facilities is necessary to prevent unauthorized use and to ensure that systems are adequately protected against natural hazards, theft and damage. Access to IT facilities shall be restricted via locks and posted signs. Authorized personnel shall be charged with safeguarding IT facility keys. Safeguarding includes not copying or lending out any IT facility keys. Custodial Agencies shall develop standards and procedures to restrict unauthorized personnel from work areas and County IT systems and resources. These standards and procedures must also include directives to limit unauthorized access during normal business hours as well after normal business hours. For example, users should position their monitor out of view of passer-bys. Rooms housing significant IT components, such as mainframes, servers, etc., must be in restricted access zones. Access to such zones must be controlled, authorized, and monitored as appropriate.

3.2 Local Access

Local access is defined as any connection to County IT resources made from a terminal, workstation, device, or system that is connected to the County network by Ethernet or any other means. Local access excludes dial-in connections, connections through Virtual Private Networks (VPNs), or any connection made through the Internet.

3.2.1 Users and Privileges

Custodial Agencies shall maintain a current list of users authorized to access IT facilities under their custody. Authorized users will access the County IT systems and resources by means of a login or "user" name and password. User names and passwords shall be a means to establish the identity of users on the system, control his or her access rights and privileges, and record the actions of authorized and unauthorized users on the system. All unattended County IT systems and resources (workstation, copiers, etc) shall be "locked" or logged off. A user name and password shall be revoked upon termination of employment or completion or removal from a project. Department Heads shall notify all appropriate Custodial Agencies regarding changes in employment status or changes in project status within the supplemental policies established by the Custodial Agencies. The term "unattended" refers to those times during work when a person absents themselves from their computer for varying lengths of time for such things as meetings, bathroom visits, etc. During such times, the appropriate operating system feature shall be used to render the unattended computer inaccessible except to someone with the proper password. Before leaving work the user must log off the network unless there is a technical situation where the computer must remain logged in.

3.2.2 Passwords

Users shall choose passwords in accordance with the "Best Practices for Password Management" in *Appendix 3* of this policy. A user is charged with protecting his or her password. A user shall not 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 immediately. A user account may be disabled or deleted if unauthorized use is detected on it. If a person wrongly uses an administrator password to access or view data that lies out of his or her normal privileges, then he or she will be subject to disciplinary action. Custodial Agencies shall adopt supplemental policies that govern passwords on the IT systems and resources in their custody.

3.2.3 Data

Custodial Agencies shall determine, following applicable regulations, County personnel who are able to access data and information under the Custodial Agencies' control. This shall be documented via a User Access Form. In general, County personnel will not be granted direct access to their own personnel records or any job related records, but shall be allowed access to these records by the custodial agency as required by law.

County data shall not be taken home or given to any unauthorized person without prior written approval of the Custodial Agencies. Non-County personnel or agencies can be granted access with prior approval via a County Access Authorization Form, which will be maintained by the Custodial Agencies.

Custodial Agencies with systems containing protected or confidential data must develop procedures that limit access to such data to authorized users only. Such procedures shall be developed consistent with all applicable laws. These procedures must describe how users become authorized, must describe how auditing is done to ensure the confidentiality of information, and must cite the appropriate laws or regulations pertaining to the management of the data.

3.2.4 Other

Custodial Agencies shall determine access rights of personnel to various IT systems and resources, such as copiers, printers, pagers, scanners, e-mail, telephones, pagers, etc. As required in *Section 3.1* of this document, Custodial Agencies shall develop procedures to restrict unauthorized users from accessing IT systems and resources during standard business hours, as well as after-hours. Custodial agencies shall establish appropriate personnel background checks that may include fingerprinting, reference checking, or other levels as necessary.

3.3 Remote Access

The County of Tuolumne encourages using remote access for departmental needs. Users who gain access to County resources through remote access methods must follow all policies of local access and, in addition, must follow the rules below.

3.3.1 Users and Privileges

User accounts shall be set up by the Information Systems and Services (ISS) department and shall restrict users from viewing or altering sensitive data. Custodial Agencies shall define the specific data and IT resources that their users have remote access to. For consistency and security, such definitions must be approved and implemented by ISS.

3.3.2 Firewalls

A user shall not send or receive data on any port that is not protected by a firewall, or bypass firewall protection in any way. Additionally, a user shall not disclose the configuration of any firewall software that protects County networks.

3.3.3 Approved Methods of Access

There is only one way in to the County network and that is through a firewall. Any other means of access to the County network is prohibited. Additionally, a user shall not bypass any network security measure to connect to the County network or County

systems using external or internal means, such as by modem. The only exception is with prior authorization in writing from the ISS Manager.

3.3.4 State Networks

Custodial Agencies and ISS shall develop policies to ensure the security of State networks, such as the California Law Enforcement Telecommunications System (CLETS), by preventing unauthorized personnel from using state networks.

4. Policy of Usage

4.1 Acceptable Use

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. Additionally, games shall not be installed on any computer that is County property, nor will gaming take place on such computers. Unacceptable uses include but are not limited to such things as non-business related e-mail, non-business related Internet surfing, and other applications which are not approved by the County.

Except for authorized investigations, users shall not use County IT resources to access offensive material on Internet sites, or otherwise send or receive offensive material. Offensive materials are any statements, jokes, comments, images, or other electronically transmitted matter that are of a sexual, racial, gender or other nature, and would violate state or federal law against discrimination or harassment based on race, religious creed, color, national origin, ancestry, physical or mental disability, medical condition, marital status, sex, age, or sexual orientation. Such offensive material includes, but is not limited to, sexually explicit or suggestive comments, jokes or images, racial, gender or ethnic slurs, or matter disparaging a person based on one of the above categories. State or Federal law refers to Title VII of the Civil Rights Act of 1964, or the California Fair Employment and Housing Act.

It is not the intent of this policy to preclude the use of IT resources for non-business related activities at appropriate times during the workday. This view must be taken into account in any department or agency level supplemental policies that arise from this policy. Department Heads and Agency Administrators can approve non-business related use of County IT systems. The authorization of any non-business related use shall be specifically described in departmental or agency supplements to this policy.

4.2 Fixed Workstations and Terminals

The use of workstations and terminals is governed by the acceptable use policy stated in *Section 4.1* of this policy. Additionally, Custodial Agencies shall appoint managers to be

held accountable for all workstations within the work area. All software on workstations needs approval by Department Heads, must be legally licensed, and must be installed by ISS. Each user will make sure that his or her workstation has standard anti-virus software installed.

All components of workstation (monitors, processor, etc) must be securely attached to furniture or walls where necessary. Surge protectors or other power line conditioners must be fitted between the computer and the main power supply. Modification of hardware configuration of any workstation components shall not be done without approval from Custodial Agencies and the concurrence and assistance of ISS. Any request for acquiring peripherals to connect to workstations shall be in accordance with County Standards as described in section 6 of this document.

4.3 Mobile Computers

Mobile computers are defined as computers that are not permanently attached to the County network. This definition includes Notebooks (Laptops), Personal Digital Assistants (PDAs), and any other computer which is considered portable. If a mobile computer is personal property of the user, it must not be connected to a County network and must not contain any data, media, or device which is the property of the County. Any mobile computer that is considered the Property of the County shall be bound by the same rules of use for fixed workstations and terminals. These computers shall not be used for non-County business, even if taken from the premises of County buildings. Unacceptable uses are defined in *Section 4.1* of this policy and include non-business related e-mail, non-business related Internet surfing, and other applications which are not approved by the County. Additionally, a user of a County-owned mobile computer may not alter its hardware configuration in any manner. If new hardware is desired (for example a memory upgrade or the addition of a wireless modem), a request must be placed to and approved by ISS.

4.4 Specific Applications

4.4.1 Electronic Mail

Electronic mail or e-mail is a valuable resource for communication and sharing data, however it is to be used with caution as e-mail allows the proliferation of sensitive or malicious data.

The use of e-mail shall be governed by the rules set forth in the beginning of *Section 4.1* of this policy. Along with these acceptable use policies, there are several e-mail-specific supplemental policies that users must follow.

Users must not open any e-mail attachment that was received from outside the County network, except if received from an external agency or individual that is exchanging information in an official capacity with the County. Additionally, all e-mail attachments must be scanned for viruses, either automatically or manually. Failure to follow these rules could result in the introduction of a computer virus into the County network.

Because of access under Section 4.7 by third-party administrators and other authorized personnel, such as supervisors and management, email is not confidential and should not be used for confidential communications.

Users shall not store e-mail messages longer than the length of time defined in the County Data Retention Policy (*see Section 6.6*), unless the message is considered a permanent document. Custodial Agencies are responsible for determining which of their data are permanent and which are temporary (*see Section 6.5*).

Users shall encrypt e-mail messages as required by their specific Custodial Agency (*see Section 6.7*).

4.4.2 Other Internet Applications

The use of Internet applications, such as web browsers, FTP clients, and Telnet clients, shall be governed by the rules set forth in *Section 4.1* of this policy. Users shall only view Internet material related to County business. Additionally, users shall not download any file that has not been approved by their Department Head. Following these rules can reduce the chance of inadvertently introducing a computer virus onto the County network.

4.4.3 County Bulletin Board

(*County Policy on Bulletin Boards will be determined at a later date.)*

4.4.4 Other Software

The use of all other software shall be governed by the rules set forth in *Section 4.1* of this policy and shall adhere to any standards set forth in *Section 6* of this policy. Furthermore, the use of software may be defined in Custodial Agency policies.

4.5 Network Services

4.5.1 Internet

The rules in *Section 4.1*, *Section 4.4.1*, and *Section 4.4.2* of this policy set forth the acceptable use of the Internet and Internet-related resources. In addition to the preceding acceptable use rules, users shall not use the Internet for gaming, chatting (such as AOL Instant Messenger or ICQ), or hacking. Additionally, Custodial Agencies should establish supplemental policies to ensure proper usage of the Internet as a work-related tool only.

4.5.2 County Network

Use of the County network is governed by the acceptable use rules in *Section 4.1* of this policy. Additionally, if a user finds that he or she can go a place or view something on

the County network that he or she should not have access to, then he or she must report this immediately to his or her Department Head or ISS. The security of the County network is under the control of ISS and in accordance with the direction of Custodial Agencies or Department Heads.

4.5.3 Other Networks

The use of other networks, such as CLETS, Health and Human Services Data Center (HHSDC), or the Library network, shall be governed by the acceptable use rules in *Section 4.1* of this policy and federal, state, or local laws. If a user finds that he or she can access networks or portions of networks to which he or she should not have access or a user notices unauthorized access to or use of a network or portion thereof, then he or she must immediately report this to his or her Department Head or ISS.

4.6 Other Equipment

Aside from the acceptable use rules in *Section 4.1* of this policy, Custodial Agencies shall establish supplemental policies to ensure proper use of IT resources such as printers, copiers, scanners, pagers, etc. These IT resources, with exception of pagers and other portable devices, may not be moved, reconfigured, or enhanced without the approval and assistance of ISS.

4.7 Privacy

All data received or sent after adoption of this policy, including e-mail and word processing documents, stored on or sent and received using County IT systems as described below and resources are the property of Tuolumne County. System administrators are authorized to examine and/or retain files within the scope of their responsibilities to troubleshoot and/or repair IT resources. System administrators shall 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. Data or the data's contents which violates the policies in this document or the law must be reported to management.

The County reserves the right to inspect, review or retain any personal electronic mail or any other personal computer data generated or received 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**.** Data on computers and network storage areas assigned by the County to Peace Officers subject to protections of the Public Safety Officer Procedural Bill of Rights Act, shall not be examined without compliance with Government Code section 3309.

Under the Public Records Act, unless a specific exemption applies, all e-mail, documents, and other information whether erased or not, may be considered public records and subject to disclosure. Such messages may also be accessed by persons involved with litigation with the County.

County IT systems include but are not limited to the following: local hard drives, servers, floppy disks, Zip disks, tape backups, and other data storage devices and media.

Notwithstanding any statements in this policy to the contrary, all employees should understand that any data and other electronic information residing on County owned equipment cannot be considered to be totally private and that authorized personnel such as supervisors and management are allowed to view it.

Any information obtained may be turned over to proper authorities for appropriate action under civil or criminal law.

5. Policy of Media and Data Storage

5.1 Handling

Media stored and handled shall be protected from physical and environmental threat. Physical and Environmental threat includes, but is not limited to, malicious or accidental damage from people, sun/heat damage, water damage, or magnetic damage. Media shall be kept out of areas with unsupervised access, locked on site, or rotated to a locked offsite facility. Custodial Agencies shall establish criteria as to where and how often their media is to be moved. Media shall be stored properly and protected while it is being moved. Custodial Agencies shall maintain records of dates, times, and locations where media is moved and stored. Media shall be clearly labeled with a description of the data it contains and the data's sensitivity level, if applicable. Media that contains sensitive information will be stored in restricted access areas and the Custodial Agencies shall determine the people who are authorized to access the storage areas.

5.2 Backups

All County sensitive, valuable, and critical data and information shall be periodically backed-up. Backup media shall be clearly labeled with the data that was backed up and the date and time the backup was made. Custodial Agencies shall establish regular back up schedules and procedures to protect all critical data.

5.3 Disposal

Any media that is disposed of that contains sensitive data must be completely erased using approved methods of erasure or must be physically destroyed. Such media should be stored in a secure location while awaiting disposal. Custodial Agencies shall document criteria and procedures describing how their media is disposed.

6. Policy of Standards

There shall be a set of standards that govern all IT systems and resources set forth by the County, ISS, and individual Custodial Agencies.

6.1 Software Standards

There shall be standards in place on software to prevent incompatibility of data between applications and to provide ease of troubleshooting and support. These standards shall include standards for word processing, Internet access applications, and virus protection. There shall be standards to ensure that virus definitions are kept up to date. And there shall be standards in place to ensure that every copy of software on County-owned IT systems and resources has a valid license.

6.2 Hardware Standards

There shall be standards in place on hardware, including computers and computer peripherals such as storage devices, printers and scanners. There will also be standards addressing copiers, pagers, cell phones, and other devices. These standards shall address among other things countywide compatibility, availability of parts and support, adherence to industry standards, and relative ease of maintenance.

6.3 Network Standards

There shall be standards in place, and maintained by the Network Services Administrator, for the creation and maintenance of County networks to ensure that malicious persons are denied access to the network and to allow ease of network maintenance. These standards shall include standards for cabling, network server software, network switches, hubs, and routers, and network security (firewalls, gateways, etc.).

6.4 Database Standards

There shall be standards, procedures, definitions, and supplemental policies in place, and maintained by the Database Administrator (DBA), ensuring that definitions for County information structures (entities, attributes, and spatial data structures) are complete, correct, and understandable, from a County-wide perspective. The DBA shall also oversee the recovery of information relating to databases. In addition, the DBA shall provide resources for the building of links to ensure access to common County information on different computer systems. Areas of joint responsibility between the Custodian and the DBA must be worked out on a Custodian-by-Custodian basis.

6.5 Data Permanency Standards

Documents, including word processing and e-mail, and data that fall outside the rules describing a document that is to be included in the Counties Electronic Document Management System or Custodial Agency/County databases are considered temporary, unless deemed permanent by the Custodial Agency or department that possesses them. Documents that are considered temporary must be deleted after a specific time, as described by the "Document and Data Retention Standards" in *Section 6.6* of this document.

6.6 Document and Data Retention Standards

There will be a County policy which sets rules for the length of time that temporary data and documents, such as e-mail, word processing, and images, are to be stored before permanent deletion. Custodial Agencies shall also set their own retention schedules based on County policy and departmental need.

6.7 Encryption Standards

Custodial Agencies shall define the standards for the use of encryption.

6.8 Training and Orientation Standards

Custodial Agencies shall develop written supplemental policies covering new users' use and access to the IT systems and resources for which they have Custodial responsibility. Specifically, standards for training shall be developed by Custodial Agencies to ensure that users have adequate skills and knowledge to properly operate IT systems and resources. These standards must include both training procedures for new workers and practices for sustaining adequate skills during the user's continued use of IT systems and resources.

6.9 Exceptions to Standards

Exceptions to standards regarding hardware or software purchases will be authorized on a case-by-case basis. To make such a determination, the department requesting the exception must present a case to both the Custodial Agency (if applicable) and the ISS Department which demonstrates that the business needs of the requesting department significantly outweigh the need for any particular standard. The ISS Department will in turn determine to what extent, if any, its resources - knowledge, equipment and software - can support said exempted item. If it is determined that the exempted item requires support by an outside vendor, such support will be coordinated by the ISS Department with all costs pertaining thereto absorbed by the responsible department.

Appendix 1 – Custodial Agency Duties

Custodial Agencies shall:

1. Determine what information is required to be collected. Data should not be collected for which there is no need.

2. Maintain plans for information collection, conversion and maintenance of data in conformity with the users needs.

3. Set the standards to determine how the information will be collected, described and used.

4. Ensure that core information requirements for the agency are met.

5. Make decisions about public access, creation of records, and fee estimates.

6. Become the authoritative source for the information under the Custodians control. This precludes confusion concerning where to go for accurate information. The custodian can then advise accurately as to the source, currency and completeness of the information.

7. Take steps to continually improve the integrity, accuracy, precision, timeliness, consistency, standardization, and value of information.

8. Define codes and edit rules to ensure completeness and integrity.

9. If part of the responsibility for data is delegated to another organization, the Custodian is still accountable for the integrity of the information. In turn, if the Custodian accepts responsibility for another agencies data, the standards of the other agency must be followed. There must be a policy in place for such delegations.

10. Provide appropriate training to staff and others to ensure data is captured accurately and completely.

11. Function as negotiator and arbitrator to achieve the best compromise in preventing or resolving conflicts in information use, interpretation, or meaning.

12. Know how other business areas affect the agency's information and conversely, know how others are affected by the agency's information.

Appendix 2 – Custodial Agency Requirements

Custodial Agencies shall:

- Document the statutory requirements and limitations associated with the data and information in their custody. (*Section 1.4*)
- Develop standards and procedures to restrict unauthorized personnel from work areas and County IT systems and resources. (*Section 3.1*)
- Maintain a current list of users authorized to access IT facilities under their custody. (*Section 3.2.1*)
- Adopt supplemental policies that govern passwords on the IT systems and resources in their custody. (*Section 3.2.2*)
- Determine, following applicable regulations, County personnel who are able to access data and information under the Custodial Agencies' control. (*Section 3.2.3*)
- Develop procedures for systems containing protected or confidential data that limit data access to authorized users only. (*Section 3.2.3*)
- Determine access right of personnel to various IT systems and resources, such as copiers, printers, pagers, scanners, etc. (*Section 3.2.4*)
- Define the specific data and IT resources that their users have remote access to. (*Section 3.3.1*)
- Develop policies to ensure the security of State networks. (*Section 3.3.3*)
- Appoint managers to be held accountable for all workstations within the work area. (*Section 4.2*)
- Responsible for determining which of their data are permanent and which are temporary. (*Section 4.4.1*)
- Develop policies to define the use of software including the County Bulletin Board. (*Section 4.4.3*)
- Establish supplemental policies to ensure proper use of IT resources such as printers, copiers, scanners, pagers, etc. (*Section 4.6*)
- Establish criteria as to where and how often their media is to be moved. (*Section 5.1*)

- Maintain records of dates, times, and locations where media is moved and stored. (*Section 5.1*)

- Determine the people who are authorized to access the storage areas. (*Section 5.1*)

- Establish regular back up schedules and procedures to protect all critical data. (*Section 5.2*)

- Document criteria and procedures describing how their media is disposed. (*Section 5.3*)

- Set their own retention schedules based on County policy and departmental need. (*Section 6.6*)

- Define the standards for the use of encryption. (*Section 6.7*)

- Develop written supplemental policies covering new users' use and access to the IT systems and resources for which they have Custodial responsibility. (*Section 6.8*)

- Develop standards for training to ensure that users have adequate skills and knowledge to properly operate IT systems and resources. (*Section 6.8*)

Appendix 3 – Definitions

Chatting – Conversing with others in real time via digital means over a network. This includes sending or receiving messages using chat-clients, such as AOL Instant Messenger, ICQ, or IRC, and using online chat rooms, such as Yahoo Chat.

Data – In computing, information, including text, images, sound, and video that is stored on computer media or carried via wire/fiber. Also, any factual information stored in any form.

E-Mail – A service that uses mail protocols such as Simple Mail Transfer Protocol (SMTP) to transfer data over a network between users. Unless a message is encrypted, it is considered not secure and could be viewed by anyone. Examples of e-mail clients include Eudora and Microsoft Outlook.

Ethernet – A standard for connecting computers together into a network.

Firewall – A network security device that can filter or block incoming and/or outgoing data or connections that pass through it. Firewalls are usually found at points of connections between a private network and a public network.

FTP – File Transfer Protocol – One of the Internet protocols used to transfer files across a network.

Gaming – Using the computer to play games. This includes Internet gaming as well as playing computer games that reside on media on a local computer.

Gateway – A bridge between two networks or between a network and the Internet. Gateways usually forward information from one network to another and filter information using firewalls or proxy servers.

Hacking – Purposeful circumvention of computer or network security for malicious purposes, sport, or the satisfaction of curiosity.

Internet – A collection of computer servers and clients across the world linked through a complex network of backbone servers. The Internet is capable of carrying such services as the World Wide Web (WWW), FTP, and e-mail.

ISS – Information Systems and Services Department, a division of the County Administration Office of Tuolumne County, which is charged with the responsibility for administering and maintaining the computer networks owned by the County of Tuolumne.

IT – Information Technology – Technology, such as computers or networks, relating to the storage, modification, and distribution of information (data).

IT Resource/System – Any device or system, which facilitates the transfer, storage, or processing of data. Examples include: computers, routers, printers, network cables, monitors, mice, keyboards.

ITSPC – IT Security Policy Committee

LDAP – Lightweight Directory Access Protocol -- software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the Internet or on a corporate Intranet.

Media – Anything that can store computer data. Examples include: floppy disks, hard disk drives, memory chips, CDs.

PDA – Personal Digital Assistant – A microcomputer, usually palm-sized, that is commonly used to organize data and track schedules and appointments.

Server – A computer program that provides services to other computer programs in the same or other computer. Example includes: Web server, mail server, FTP server. Also, the computer on which the computer program runs.

System Administrator – Any person who is authorized by the County and ISS to perform system configuration, maintenance, and repair. System Administrators have a higher level of system access than typical users.

User – Any employee, permanent or temporary, contractor, consultant, vendor, elected official, volunteer, student, or other person who uses, maintains, manages, or is otherwise given access privileges on the County's IT systems.

User Account- That account which is set up by the Network Administrator and which when accessed by a username and password provides access to County Network resources such as printers, file storage and email.
Virus (Computer Virus) – A virus is a piece of programming code usually disguised as something else that causes some unexpected and, for the victim, usually undesirable event and which is often designed so that it is automatically spread to other computer users. A computer is "infected" when a virus or infected program has been run on that computer. Viruses usually come attached to programs or imbedded in word processing documents which support macros.

VPN – Virtual Private Network – Private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures

World Wide Web (WWW) – The collection of servers that are using the Hyper Text Transfer Protocol (HTTP) over the Internet to distribute data. Unless encrypted, the submission of data across the WWW is considered not secure and could be viewed by

anyone. Examples of Web clients (Browsers) include Netscape Navigator and Microsoft Internet Explorer. Examples of Web servers include Apache, and Microsoft Web Server.

Appendix 4 – Best Practices for Password Management

Select Good Passwords

Good passwords should be easy to remember, but hard for others to guess. Intruders can 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 guess or extract.

- 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.
- 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 software doesn'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 thus 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 or extract.

- 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, pet's names, relative's names, or 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 such as "start", "start-it", "start-up", "open", "open-up", "opensesame", "opensezme", "its-me", "let-me-in", "access", or "access-it".
- DON'T use obvious, job-related terms such as "tuolumne", "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 English-speakers, 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.

NOTE: Avoid using script files, macros and options with embedded passwords to automate your login process.

Don't allow password boxes that are filled in with your password to be left open. It is very easy to reveal a password in a password box, even if it appears masked by asterisks or any other symbol.

Passwords Management for Different Systems

Unless you are a user on a system designed for a single login, such as an LDAP-compliant system, 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).

If you are a user on a system designed for a single login, you should follow the rules for your system. It is also important to change your password frequently.

Attachment 1 - Acknowledgement Of Information Security Responsibility Form

COUNTY OF TUOLUMNE

ACKNOWLEDGEMENT OF
INFORMATION SECURITY RESPONSIBILITY

I,_____, acknowledge that the purpose of the County's information technology network including its computers, telephones, pagers and other resources is to support County business. Employees shall not 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. Furthermore, the conditions described in this policy for any authorized non-business related use of IT systems will be contained in the employee's departmental policies.

The County reserves the right to audit, access, and review all matters on the County's information systems 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. The use of a County-provided password 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.

Employees who violate this policy may lose any access privileges granted by the County and be subject to disciplinary action up to and including termination or, in the case of a non-County employee, termination of their contract.

I acknowledge that I have received and read the County's Information Technology (IT) Policy and this acknowledgement.

_____ _____

Signature Date Signed