



TRINITY COUNTY
PERSONNEL POLICY

SUBJECT:	INFORMATION TECHNOLOGY (IT) POLICY
POLICY NO.:	16-01
INITIAL DATE PREPARED:	2/2000
LAST DATE REVISED:	February 17, 2016
RESOLUTION NO.:	N/A

TABLE OF CONTENTS

I.	PURPOSE	2
II.	APPLICABILITY.....	2
III.	DEFINITIONS	2
IV.	SOFTWARE PURCHASING AND LICENSING POLICY	2
III.	HARDWARE PURCHASING POLICY	3
IV.	COMPUTER INFORMATION TECHNOLOGY SECURITY POLICY	4
V.	E-MAIL AND ELECTRONIC DATA POLICY.....	6
VI.	INTERNET POLICY	7
VII.	NON-COMPLIANCE	7
VIII.	DEVIATION POLICY	7
IX.	EMPLOYEE SIGNATURE STATEMENT	7

I. PURPOSE

The purpose of this policy is to set forth Trinity County's policy regarding hardware and software purchasing, software licensing, internet usage, e-mail usage and security.

II. APPLICABILITY

This policy applies to all County employees, volunteers, interns, vendors, and contractors, as well as to all applicants for such positions.

This policy applies to all personal computers and wireless devices.

This policy shall not be interpreted or applied in any manner that would be inconsistent with any applicable state or federal law or regulation, or increase the legal liability of the County.

III. DEFINITIONS

1. Data - any and all files (spreadsheet, document, image, etc.) that are stored either on shared network resources and/or local storage. Storage shall include both fixed devices and removable media.
2. Email - any and all electronic communication initiated and/or received by County systems.
3. Freeware - computer software that may be distributed and used without payment.
4. Hardware - the physical parts or components of a computer, such as the monitor, mouse, keyboard, computer data storage, hard disk drive (HDD), graphic cards, sound cards, memory, motherboard, etc., all of which are physical objects that are tangible.
5. Personal Computer - a microcomputer designed for use by one person at a time.
6. Primary User - the person, group, or other entity which is charged with maintaining an information asset on behalf of Trinity County.
7. Shareware - computer software that you can try for free for a certain period of time before choosing whether or not to buy it.
8. Software - any set of instructions that directs a computer to perform specific operations. Computer software consists of computer programs, libraries and related non-executable data (such as online documentation or digital media).
9. Wireless Devices – A device that uses a wireless protocol (802.11a, b, g, or n) to connect to the Internet or a private network.

IV. REQUESTING SERVICES

All service tickets for the Information Technology (“IT”) Department should be done through submission to the helpdesk at helpdesk@trinity county.org.

Department Heads with confidential or sensitive matters are instructed to contact the IT supervisor by telephone or personal email.

V. SOFTWARE PURCHASING AND LICENSING POLICY

1. Introduction. Trinity County purchases or licenses the use of copies of computer software from a variety of outside companies. The County does not own the copyright to this software or its related documentation. The County only has the right to reproduce the software or related documentation as authorized by the software vendor. The County does not condone the illegal duplication of software.
2. Objectives. With regard to use on County computers, Trinity County employees shall use software only in accordance with the terms of that software’s license agreement.
3. Guidelines. Trinity County employees learning of any illegal use of software or related documentation within the County must immediately notify their supervisor or department head.

The following is Trinity County’s policy regarding specific components of software management:

- a. Software Not Authorized by Trinity County - The download and installation of shareware and freeware by County employees requires written approval via email from the employees’ Department Head and the IT Department’s Help Desk. Installation of any game is prohibited on County computers. Software applications cannot be brought from home and loaded onto a County computer. It is Trinity County’s policy that the County may conduct random audits to verify that every application used within Trinity County is a legal copy. Any programs that are found to be illegal and in violation of this policy will immediately be removed from the system. An employee’s use of unauthorized software or unapproved shareware or freeware may result in disciplinary proceedings against that employee, up to and including termination.
- b. Software Acquisition Process - Each department shall work with the IT Department to determine its needs. Because software is expensive and is a critical part of the information technology, each department shall work with IT Department in order to ensure the success of the application’s specifications, procurement, development, deployment, and support. The IT Department will then work with each Department in fulfilling the specified requirements. Software packages may be evaluated by Department to determine which is best for the specific office, if such

evaluation is allowed by the publisher. All copies of the evaluation software must be removed from the computer within the specified time limitations.

- c. Installation - All software installation will be done by the Trinity County IT Department. This is to aid in the elimination of problems associated with printer set-up, software and hardware compatibility, and correct application of system defaults.
- d. Virus Check - All workstations, Personal Computers ("PC), and laptops connecting to the Trinity County Network shall meet the following requirements:
 - i. Have an antivirus program installed and up to date.

Systems that do not meet these criteria shall be quarantined until the required software and patches are installed. While in quarantine, the system will not be able to connect to any County resources. Any removable storage device (defined as USB hard drives, thumb drives, flash drives, or any other type of data storage device) that has been used on a computer system outside of the Trinity County Network shall be checked for viruses by the user before being used on a workstation or server on the County Network. The media of all new software shall be checked for viruses before being used or installed on a workstation or server on the County Network.

VI. HARDWARE PURCHASING POLICY

1. Introduction. Trinity County purchases computer hardware from a variety of outside companies. The IT Department continually monitors and reviews the computer industry and the tools of Information Technology, always mindful of the County's need for products capable of high performance, reliability, compatibility, and return of investment.
2. Objectives. Trinity County has several objectives in mind when acquiring computer hardware. A significant goal is to reduce incompatibility problems. Other goals include reducing administrative costs associated with the acquisition of IT hardware, reducing implementation time and complexity, improving management and control, improving quality and reliability of purchases, improving economy of scale, and improving the budget planning process, which enhances the total cost of ownership.
3. Guidelines
 - a. Hardware Acquisition Process - Because hardware is expensive to purchase and maintain, and also performs a critical role in maintaining application availability and security, IT provides guidelines for hardware purchasing decisions. It is important that the County acquire

hardware that meets our applications' requirements, is reliable, has reasonable life expectancy, is readily serviceable, supportable, and compatible with our network and security requirements. It is also important to reduce the Total Cost of Ownership, and choose vendors that are flexible and responsive to the County's changing Business needs.

Offices planning to purchase hardware which may be connected to the County Network, or eventually require IT Support, shall notify the IT Department early in the procurement process and prior to procurement.

- b. Installation - All networked computer hardware installation is to be done by the IT Department.

VII. COMPUTER INFORMATION TECHNOLOGY SECURITY POLICY

1. Introduction. Computer information security is the responsibility of each County Employee and contractors/vendors working with County information. Computer information security is the protection of information assets. Information assets are protected from accidental, intentional, unauthorized disclosure, and modification or destruction, including temporary loss of availability of information assets.

Information assets are computer hardware, software, and data that is owned, leased, managed, or used by Trinity County. All application software, information in databases or files, information in handwritten, typed, pictorial, digital or analog form, operating system software, utility programs, printouts, storage media, and their contents, terminals, data communication devices and computers are examples of Trinity County's information assets.

2. Objectives. The objective of this policy is to safeguard Trinity County information assets. This policy will define information security, classification of information assets, who is responsible and the consequences of non-compliance.
3. Guidelines. All Trinity County employees, contractors and vendors are responsible for protecting the County's information assets. County employees learning of any breach of information security within Trinity County shall immediately notify their respective supervisor or department head. Trinity County employees are required to comply with all information security policies or be subject to discipline, up to and including termination.
 - a. Physical Access - Access to the main computer room is restricted to authorized personnel.
 - b. Personal Computers – Employees are prohibited from using their personal computers and wireless devices for county related matters.
 - c. Data Access - To insure maximum information security, Trinity County administers computer security under the program of “least

amount of privilege to perform their job.” Each user will be given the rights to access only the information necessary to perform the duties of their position. Each computer device must have its own device ID.

- d. Unattended Computers - All computers must be locked at night or when left unattended. Prior to turning-off a computer, all applications and the operating system will be shut down according to the guidelines published by the software manufacturer. All PCs must be logged-off at night or when left unattended for an extended period of time.
- e. Use - All data residing on County systems is the property of Trinity County and its representatives and is to be used by and for Trinity County for county purposes only. Likewise, all email communication initiated and/or received by the County systems is the property of Trinity County and its representatives and is to be used by and for Trinity County purposes only.
- f. Personal and Account Password Control - Passwords are used to verify that the user of an ID is the owner of the ID. The ID-password combination is unique to each user and therefore provides a means of holding users accountable for their activity on the system. Therefore, under no circumstances are IDs and passwords to be shared, (this includes the employee’s supervisor or department head), or written down and placed in a visible location on or around the computer or desk.
- g. Data Storage - The IT Department does not backup local hard drives. Trinity County workstations are configured to store data files on assigned network drives. These assigned network drives are backed up each night. If a local hard drive malfunctions, the data is lost and cannot be recovered by the IT Department.
- h. Attachment To The Trinity County Network By Outside Agencies - All connections to public or unsecured networks, such as the Internet, must have firewall protection.

Any outside agency wishing to directly attach to the County network must have a contract signed by The Board of Supervisors of Trinity County and the “Primary User” of the data to be accessed. Prior to making a direct network attachment, the requesting agency must agree to conform to this IT policy statement. The County will have the right to ensure conformity with this policy.

Trinity County reserves the right to deny any application for direct connection to the County network.

Trinity County further reserves the absolute right to terminate the agency’s direct network attachment for any reason. No property right is received when attachment is allowed. It is merely a revocable privilege.

- i. Data Disposal - Disposal of data storage media is handled in a secure manner. Disk drives, diskettes, tape reels and cartridges, and other such media must be erased before they are transferred to new ownership. If they are being disposed of they must be damaged such that their contents are rendered unreadable. The largest opportunity for information leakage occurs in the disposal of printed reports. Particularly because Trinity County is recycling a large volume of paper, care must be taken to render unreadable any report or document that carries a moderate or high risk. The disposal of any document at the County is subject to rules governing County records retention.
- j. Computer Virus Detection - County employees will report all instances of computer virus to The IT Department immediately. Anti-virus software must be installed on all Trinity County computers that have the potential to be connected to the network in order to detect, identify, isolate, and eradicate viruses unless there is written permission by IT. This software must be updated to fight new viruses. In order that the viruses are intercepted as early as possible, the software will be kept active on a system, not used intermittently at the discretion of users.

Any computer which is identified as containing a computer virus will be subject to immediate correctional measures. This includes virus checking all media and all computers which may have shared portable media with the infected computer.

- k. Personnel - Department Head is responsible for notifying IT, via the helpdesk, of change in employee employment status. IT personnel are then responsible for disabling or revising any accounts used by the former employee. The IT Department should be notified of any new employees at least 24 hours before the new employee reports to work.
- l. Data Breach – If any employees are aware of a data breach they are to report this to their supervisor immediately. The supervisor shall immediately report this information to Risk Management and the IT Department.

VIII. E-MAIL AND ELECTRONIC DATA POLICY

1. Purpose. The purpose of this policy is to explain the proper use of e-mail and electronic data. Use of e-mail on County computers is to provide business-related communications. Trinity County policies that apply to paperwork also apply to electronic data and e-mail (ref. Data Disposal section).

Trinity County computers are provided to employees for the sole purpose of facilitating the work of the County and its agencies. Employees have no right to privacy with regard to their use of the County computer system and computers including the use of e-mail and internet. The County does not waive any privileges, including those provided by statute, rule or common law. Passwords are not indicative of privacy, rather a password is a security tool used on behalf of

the County. E-mail communications can and may be monitored. Therefore, the County encourages its employees to refrain from using the County computer system for transmission of personal information and communications.

2. Appropriate Usage. Appropriate usage of e-mail is for business-related communications. Prohibited usage includes, but is not limited to, distribution of chain letters, inappropriate humor, offensive graphics and images or language that may offend someone on the basis of age, race, sex, religion, national origin or disability.
3. Monitoring. E-mail may be monitored, upon request of or with the permission of an employee's Department Head, for personnel purposes.
4. Internet Transmission of E-Mail or Electronic Data. All employees are prohibited from transmitting over the internet any County information and/or electronic data that is regarded as privileged or confidential without first securing a method of protecting the data. If there is a doubt as to whether information is privileged or confidential, or as to whether a transmission will utilize the internet, employees are required to discuss the issue with their supervisor before transmitting.

IX. INTERNET POLICY

1. Introduction. Internet access on County computers is a privilege extended to some of the County's employees. Proper usage of the internet is the responsibility of each Trinity County employee. Use of the internet on County computers is provided to employees for the purpose of facilitating the work of the County and its agencies and only from the authorization of the supervisor or department head.
2. Privacy. Employees have no right to privacy with regard to their use of the internet on County computers. Internet usage may be monitored.
3. Appropriate Usage. Appropriate usage of the internet is for business-related activities. Prohibited sites include those containing offensive graphics, images, and language. Streaming or downloading of files without approval of a Department Head, after consultation with the IT Department, is strictly prohibited.
4. Incidental Personal Use. The County strongly discourages employees from using their County computers or wireless devices to conduct personal emails, pay bills on-line or use the internet. If an employee needs to use their County computer or wireless devices for personal use, they should get permission from their Department Head.

X. NON-COMPLIANCE

All policies are in full force and effect both during and after working hours. Non-compliance with these policies may result in formal disciplinary proceedings, up to and including, termination or the permanent cancellation of computer privileges.

XI. DEVIATION POLICY

There shall be absolutely no deviation from this policy without the written authorization from the IT Department and the Department Head. Any deviation without said written authorization shall be considered non-compliance.

XII. EMPLOYEE SIGNATURE STATEMENT

All employees will read and sign a Trinity County Computer Policy Statement before being given computer access privileges.

DULY PASSED AND ADOPTED this 17th day of February, 2016 by the Board of Supervisors of the County of Trinity.

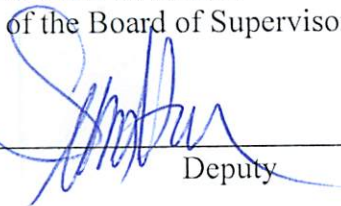


L. KARL FISHER, CHAIRMAN
Board of Supervisors
County of Trinity
State of California

ATTEST:

MARGARET E. LONG
Clerk of the Board of Supervisors

By: _____



Deputy