Summary of the
Information Technology (IT)
Security Policy

Tulare County Department of Information Technology

County Civic Center 221 S. Mooney Blvd.

Service Desk: 636-IT4U

Summary of the
Information Technology (IT) Security Policy

Information Technology Security Program: Adopted April 6, 2010 by the Tulare County Board of Supervisor Resolution No. 10- 0259 effective for all Employees.

<u>Rule # and Rule</u>

1.1 Purpose

The purpose of this policy is to define general information security responsibilities for every User of County Computing Assets, and establish a documentation structure for the appropriate access to, and integrity of, County Computing Assets (see DEFINITIONS).

1.2 Scope

The County Information Technology Security policy serves as the minimum standard to which all departments must adhere. Additional policies addressing specific areas of information security also exist (see the full listing under RELATED DOCUMENTS/POLICIES.) Individual departments may implement additional written information security policies to meet their business needs as long as the departmental policies are consistent at all times with the County policies. These policies cannot be overridden or altered by any informal practice of an agency or department or by statements of supervisors or managers within a department.

1.3 Policy

1.3.1 Overview

County Computing Assets must be appropriately used, evaluated, and protected against all forms of unauthorized access, disclosure, modification, or denial. Security and controls for County Computing Assets must be implemented to provide:

1.3.1.1 Privacy and confidentiality – prevent unauthorized disclosure of systems and information.

1.3.1.2 Authentication – verify the identity of the sender and/or receiver ofinformation.

1.3.1.3 Data integrity – prevent unauthorized modification of systems andinformation.

1.3.1.4 Availability – prevent disruption of service andproductivity.

1.3.1.5 Accountability – ensure correct use of the application and individual responsibility of that use.

1.3.1.6 Audit ability – provide the ability to review/analyze logged security events both at the system and application software levels.

1.3.1.7 Appropriate use – ensure Users conform to County rules, ordinances and policy, and state and federal law.

1.3.1.8 An electronic copy of this can be found on the Tulare County Intranet under Information Technology and under Human Resources & Development.

1.3.3 User responsibilities:

1.3.3.1 Understand and adhere to County information security policies as well as appropriate organizational policies.

1.3.3.2 Protect the County Computing Assets with which they are entrusted and use them for their intended purposes.

1.3.3.3 Sign an Acceptable Use Policy Acknowledgement as a condition of being granted access to County systems (Form attached to this document).

2.1 Purpose

The purpose of this policy is to outline the acceptable use of County Computing Assets (see DEFINITIONS).

2.2 Scope

This policy applies to all Users of County Computing Assets. Each User has a responsibility to use County Computing Assets in a manner that increases productivity, enhances the Company's public image and is respectful of others. Inappropriate use exposes the County to risks and threats to telecommunications, information systems, networks, facilities, and legal issues, and failure to follow the County's policies regarding its technological resources may lead to discipline, up to and including termination from employment.

2.3 Policy

2.3.1 Overview

2.3.1.1 The County is committed to protecting itself from illegal or damaging actions, whether by intentional or unintentional means.

2.3.1.2 County Computing Assets are provided for conducting County business.

2.3.1.3 Effective security is a team effort involving the participation and support of every User of County Computing Assets. Every User must know this policy and conduct his/her activities in compliance with it.

2.3.1.4 A full listing of County Information Technology Security Program Policies is listed under RELATED DOCUMENTS/ POLICIES.

2.3.2 General Use and Ownership

2.3.2.1 The County or department-authorized individuals may conduct audits or investigations of its Computing Assets to monitor usage, or to otherwise ensure compliance with this policy or department-specific policies.

2.3.2.2 Nothing in this section will change the legal status of confidential or privileged information.

2.3.2.3 Users should be aware that the data they create on County Computing Assets is the property of the County, unless the legal ownership is otherwise defined by law, as in confidential or privileged information.

2.3.2.4 All Users acknowledge that there is no personal right of privacy for the User using County Computing Assets. The use of a password does not create a right to privacy.

2.3.2.5 Authorized individuals within the County may monitor equipment, systems, and network traffic at any time for security, network maintenance, policy compliance or other purposes.

2.3.2.6 All Users shall use County Computing Assets in compliance with all applicable federal, state and local telecommunications and networking laws and regulations and County policies and procedures

2.3.2.7 All Users shall report known or suspected inappropriate use or abuse of County Computing Assets to the appropriate Department head and/or other County incident reporting resource.

2.3.3 Electronic Mail

2.3.3.1 County provided Internet E-mail sent to, or received from an Internet address, may be reviewed for various reasons. For example, if undeliverable for a variety of reasons, may have its contents reviewed for the purpose of determining addressability.

2.3.3.2 County provided virus protection will be maintained for all inbound and outbound E-mail. If possible, when an infected message is detected at the mail server, the virus protection software will attempt to clean it. If unable, it may delete the infected attachment or the entire message if needed to remove the virus. When an infected message is detected, a notification will be sent to the recipient and the E-mail administrator regardless of whether the message is cleaned or deleted.

2.3.3.3 Message backup occurs by duplicating all messages and creating a storage copy. This procedure is performed nightly and held for 60 days. When authorized, messages can be restored from a backup copy. These procedures are intended for disaster recovery purposes, and not for user convenience.

2.3.4 Use of County Provided Computer Assets for Personal Use

2.3.4.1 The County provides Internet services, E-mail services, telephone services, and computers to enable Users to con- duct the County's business in an efficient manner. Only employees whose job performance will benefit from the use of County Computing Assets will be given access to the necessary technology. These services and hardware systems are to be used in the direct conduct of the County's business.

2.3.4.2 Users may occasionally use County provided Internet services, E-mail services, telephone services, and computers for incidental personal use at the discretion of their department head or their designee, at approved times, provided it does not interfere with the performance of work duties, does not otherwise conflict with County business, is not done for pecuniary gain, and is in accordance with all applicable policies. Users may only engage in such use during non-work (unpaid) time. Incidental use may be to send and receive necessary and occasional personal communications; prepare and store incidental person data (such as personal calendar appointments, address lists or similar incidental personal data) in a reasonable manner; to use the telephone for brief and necessary personal calls; and to access the internet for brief personal use. The User must limit his/her use so that the County's equipment is available for County use. The standard will be "reasonable use" as defined in the definitions section of this document. County assumes no liability for loss, damage, destruction alteration, disclosure or misuse of personal data or communications transmitted by or stored on County Computing Assets. These acceptable uses identified are not exhaustive but an attempt to provide a framework for activities that fall into the category of acceptable use. Therefore, certain activities or usage may be deemed unacceptable by a department head.

2.3.5 Security and Proprietary Information

2.3.5.1 Information contained on Internet/Intranet/Extranet-related systems is either confidential or public, as defined by organizational confidentiality guidelines. Examples of confidential information include, but are not limited to: medical in- formation, personnel information, User data, vendor and bidder sensitive information, specifications, and other data. Users should take all necessary steps to prevent unauthorized access to this information.

2.3.5.2 All County Users must acknowledge (by signing a form) having received the County's Acceptable Use Policy (ATTACHMENT) annually, and are assigned accounts for their specific use based on their defined needs. Passwords are required to enable Users to keep their County Computing Assets secure. Users are responsible for the following:

a) The security of their accounts.

b) Not sharing their passwords.

c) Changing their password in accordance with individual application requirements.

2.3.6 Recommended Security Technologies

2.3.6.1 Password-protected screensavers, with automatic activation set at 10 minutes or less (of inactivity), are recommended on all PCs, laptops, and workstations.

2.3.6.2 Personal Digital Assistants (PDA) or other very portable digital equipment should power down and/or automatically be secured at 5 minutes or less when inactive.

2.3.6.3 It is recommended that Users log off the network when their workstations will be unattended for extended periods of time. All devices must require password re-authorization when re-activating.

2.3.6.4 Use encryption, when/where available, for information that Users consider sensitive or vulnerable in compliance with established departmental standards and State and Federal guidelines as appropriate.

2.3.6.5 Because information contained on portable computers is especially vulnerable, exercise special care in the handling, storage and transportation of this equipment.

2.3.6.6 All computers that are connected to the County Internet/Intranet/Extranet, whether owned by the User or County, must continually execute approved virus-scanning software with a current virus database (See Virus Protection Policy).

2.4 Unacceptable Use

Users may not use any of the County's Computing Assets for any illegal purpose, violation of any County policy, in any way that discloses confidential or proprietary information, or in a manner contrary to the best interests of the County. The following activities are prohibited except as required in the performance of a User's duties. The four lists below (system activities, network activities, email & communication activities, and other activities) are not exhaustive but attempt to provide a framework for activities that fall into the category of unacceptable use.

2.4.1 System Activities

2.4.1.1 Any purpose which violates applicable federal, state or local telecommunications or networking laws or regulations or County policies or procedures is strictly prohibited. County reserves the right to determine the likely legality, appropriateness, business relevance or unethical nature of any use or of information residing on its system.

2.4.1.2 Using a County Computing Asset to knowingly engage in viewing, reading, creating, conveying, downloading, transferring, transmitting, scanning, or printing any of the following:

a) Illegal, Defamatory, Offensive or Discourteous content of any kind, including pornographic material, for any purpose, including sexual gratification or humor, and including sexually explicit images, messages, websites, jokes, cartoons, etc. or written, verbal or visual works or conduct that treat sex in an objectionable or lewd or lascivious or humorous manner and including any illegal Matter (including child pornography) or sexually explicit images deemed by community standards to be obscene.

b) Any Harmful Matter or Obscene Matter as those terms are defined in California Penal Code sections 311 and 313, which can be found on the State of California, Office of Legislative Counsel's Website: http://www.leginfo.ca.gov/calaw.html

c) Any Matter in a manner that violates the Tulare County Policy Against Harassment, Discrimination or Retaliation.

d) Content which is inappropriate in an office environment

e) Solicited or unsolicited personal views of a social, religious, political, or racial nature

f) Threatening or violent behavior, including but not limited to materials related to hate speech, illegal weapons, or terrorist activities

g) Conduct or participate in gambling activities

h) Maintain or engage in a personal/private business, outside employment or other commercial activities, including assisting another person or entity to do so

i) This provision does not apply to some law enforcement and/or other County employees in situations where they are engaging in such activities in the performance of their job duties. Department heads are required to submit a list to the Tulare County Information Technology (TCIT) Director if they have any staff that requires an exception to this provision.

2.4.1.3 Using products that are not appropriately licensed for use by the County or the user or those that violate the rights of any person or organization protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software.

2.4.1.4 Abuse, damage, or exploitation of County Computing Assets.

2.4.1.5 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copy- righted software for which the County or the User does not have an active license.

2.4.1.6 Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws is illegal. Consult the appropriate management prior to exporting any material of this nature.

2.4.1.7 Exporting, exploiting, sharing, or using for personal gain, data contained within County Computing Assets, with a private enterprise, the public, or other Users without permission of the data owning department. This includes Users developing applications or accessing data for their own department, or another County department.

2.4.2 Network Activities

2.4.2.1 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the User is not an intended recipient or logging into a server or account that the User is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to, Network Sniffing, Pinged Floods, Packet Spoofing (see DEFINITIONS), denial of service, and forged routing information for unauthorized purposes.

2.4.2.2 Executing any form of network monitoring that will intercept data not intended for the User's workstation, such as port scanning or security scanning is expressly prohibited.

2.4.2.3 Circumventing or mimicking (Spoofing) User authentication or security of any host, network, or account.

2.4.2.4 Interfering with or denying service to any Computing Asset other than the User's own workstation (e.g., denial of service attack).

2.4.2.5 Using any program/script/command or sending messages of any kind, with the intent to interfere with or dis- able any Computing Asset, by any means, locally or via the Internet/Intranet/Extranet.

2.4.2.6 Providing information about, or lists of, County Users to parties outside the County, for other than authorized County business purposes.

2.4.2.7 Adding any networked component that is connected either directly to the County's Wide-Area-Network, or indirectly connected via a Local-Area-Network segment that creates the potential for a breach of the County's network.

2.4.2.8 Accessing peer to peer audio or video streaming for personal use.

2.4.3 E-mail and Communications Activities

2.4.3.1 Sending unsolicited E-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (i.e. E-mail spam).

2.4.3.2 Any form of harassment or discrimination via E-mail, telephone, or paging, whether through language, frequency, or size of messages.

2.4.3.3 Creating or forwarding "chain letters," "Ponzi," or other "pyramid" schemes of any type, pornography or fraudulent E-mail as listed on the Federal Trade Commission's Website:

http://www.ftc.gov/bcp/menus/consumer/tech/spam.shtm

2.4.3.4 Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups, effectively producing newsgroup spam.

2.4.3.5 Accessing another employee's email or voicemail without authorization.

2.4.3.6 Transmitting or posting defamatory, obscene, offensive, threatening or harassing content in discussion forums, message boards, blogs, photo and video uploading, sharing, tagging, social networking (for example: Facebook, MySpace, YouTube, Twitter) and public discussion features. Content transmitted electronically may negatively reflect upon the County, or may be inaccurately perceived as reflecting the official County position because of transmission by or using County Computing Assets.

2.4.4 Other Activities

2.4.4.1 Downloading of personal use files to network drives such as music, pictures and movies. Do not stream audio or video over the internet, unless required to do so in the performance of your job.

2.5 County Access, Review, Deletion and Disclosure

2.5.1.1 County has the capability to access, review, copy and delete any messages sent, received or stored on County Computing Assets.

2.5.1.2 County reserves the right to access, review, copy or delete all such information for any purpose and to disclose it to any party it deems appropriate, unless such disclosure is proscribed by law.

4 E-mail Retention Policy

4.3.1.3 Even though most County e-mails may not constitute "official records," such County e-mails are probably "public records" within the meaning of the Public Records Act, and could eventually have to be disclosed to outside parties or in a court of law.

4.3.5 Possible Consequences of Identified Misuse

4.3.5.1 Observance of these policies and departmental procedures is essential to the delivery of County services and programs, and to the integrity, security, and confidentiality of County data/information. Violation of these or other policies related to County data/information and/or information systems may result in any or all of the following:

a) Reporting of the incident(s) to management.

b) Possible revocation of access privileges.

c) Possible disciplinary action, up to and including termination.

9 Logon Warning Banner Policy

9.3.1 Overview

This document establishes the County policy that all communications equipment capable of displaying system messages, must display, as the first message seen by the user, a warning that the system being accessed is a County Information Technology user.

This system is for authorized use only.

Your activities may be recorded and monitored.

You have no right to privacy while using this system.

Your unauthorized or illegal use may be a Felony Offense punishable under the

United States Penal Code, Title 18, Section 1030, the Computer Fraud and Abuse Act of 1986, California Penal Code Section 502 and other state or federal laws.

Pressing any key will continue logging in and by doing so, you accept these terms!

10 Password and Authentication Policy

10.3.2 County Minimum User Level Password Standard

Passwords shall consist of at least six or more characters. The password will include at least one numeric, one lower-case, and one upper-case character. Passwords will be changed every 180 days, and are not to be re-used. Additionally, after three incorrect attempts to enter the correct password, the Userid shall be locked-out on the fourth attempt, resulting in a minimum lockout time of 30 minutes before allowing the process to start over. These standards are employed to prevent Brute-force manual and Dictionary automated logon attempts.

10.3.3.7Passwords shall not be written down unless stored in a locked safe for recovery purposes.

10.3.6 User Password Protection

10.3.6.1Do not use the same password for County accounts as for other non-County access (e.g., personal Internet Service Provider (ISP) accounts, financial accounts, etc.)

10.3.6.2Never use the "Remember Password" feature of applications.

10.3.6.3Do not share County passwords with anyone, including administrative assistants, or family members.

10.3.6.4Do not share your password with co-workers while on vacation.

10.3.6.5If someone demands your password, refer them to this policy and your department head.

13 Privacy and Confidentiality Policy

13.4 General Non-Disclosure Statement

"The information contained in this e-mail / fax may contain information protected by the constitutional right of privacy and/or other protected privileges, including the attorney-client and governmental privileges. It is intended only for the use of the individual(s) named in this e-mail / fax and the right to privacy and other privileges are not waived by virtue of this having been sent by e-mail / fax. If the person actually receiving this e-mail / fax or any other reader of this e- mail /fax is not a named recipient or the employee or agent responsible to deliver it to a named recipient, any use, dissemination, distribution or copying of the communication is strictly prohibited without the prior written authorization from the agency or the holder of the right. If you have received this communication in error, please immediately notify us at the above e-mail address or telephone number and destroy all copies immediately."

14 Remote Access Policy

14.1 Purpose

To establish policy for allowing only authorized access to the County's computer network from a location that is not physically connected to the County's Wide Area Network (WAN) / Local Area Network (LAN).

14.2 Scope

This policy applies to all Users that have been granted remote access ability by their respective departments for the purpose of conducting County business.

14.3.1 Overview

14.3.1.1 All remote access to the County WAN will be accomplished via a secure method, i.e., strong authentication and encryption.

14.3.1.2 Access from a remote site to a County network that contains data classified as For Official Use Only (FOUO) may require extended identification and authentication procedures. (See the ITSP Privacy and Confidentiality Policy, Section 13)

14.3.1.3 All Users remotely accessing the County network will exercise due diligence in ensuring that County Computing Assets, and non-County computer systems used for this purpose, are free from viral infections and unauthorized use.

14.3.1.4 When a (previously) authorized remote User separates from County employment, is placed on administrative leave, or retires, all existing remote access services will be terminated. TCIT should be contacted as soon as the department knows of the termination so remote access to data and systems can be revoked at the same time as the termination. For voluntary (planned) terminations or retirements, TCIT should be contacted at least three business days prior to the separation so remote access to data and systems can be revoked appropriately. Interdepartmental transferees will only have their department-specific resources terminated.

14.3.2 Use and Awareness

14.3.2.1 Remote access is considered a privilege, and can be revoked at any time without cause by the authorizing department head.

14.3.2.2 State of California applications such as DMV, MEDS, and CLETS may not be permitted from remote locations due to State security regulations.

14.3.2.3 Remote sessions that are inactive for more than 30 minutes shall be discontinued automatically.

14.3.2.4 Based on the job function within the County, some departments may find it necessary and beneficial to supply County Computing Assets for use in supporting their applications remotely. If County Computing Assets are to be removed from the County premises, Users must complete an appropriate Authorization for Removal of County Computing Assets form. It must be signed (authorized) and kept on file in their department.

54 14.3.2.6 Support will be provided only for County Computing Assets used for remote service. Support will be accomplished by the end User bringing the assigned County Computing Assets to a Tulare County facility. Personal computing assets used for remote access will not be serviced by the County. The County will not be liable for damage to personal computers nor the data stored on them.

14.3.2.7 Three unsuccessful attempts to sign on to the remote facility due to an incorrect Userid or password shall result in the temporary revocation of the account. Users must call TCIT to have their logon reset.

14.3.2.8 Application forms and instructions for remote access are available from Information Technology.

Virus Protection Policy

Exercise caution when opening attachments from E-mail, Instant Messaging, etc.

17.3.2.5 Users remotely accessing the County network must exercise due diligence in ensuring that the County Computing Assets, and non-County computer systems used for this purpose, are free from viral infections. See the Information Technology Security Program Remote Access Policy for more information.

Enforcement

Any User of County Computing Assets, found to have violated this policy may be subject to appropriate disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil.

Definition of Technical Terminology

AGENCY

For the purposes of confidentiality and privacy, Agency means those persons and their supervisors within a department who have a need to know to perform their duties pertaining directly to the subject matter.

BRUTE-FORCE ATTACKS

A Brute-force attack attempts to log into a system with a known user account name by repeatedly trying different password combinations. Locking-out the User after a predetermined number of failed attempts is the best deterrent to this type of attack.

BUSINESS CONTINUITY PLAN (BCP)

Business Continuity is the ability to maintain the constant availability of critical IT systems, applications, and information across the enterprise.

BUSINESS IMPACT and RISK ANALYSIS

Define the many potential disruptive threats to a department's Information Technology including environmental, de- liberate, utilities, etc., and their short- and long-term impact on the business processes.

BUSINESS RECOVERY

Defines the steps required to recover from a situation that had some impact on the department's normal IT

functions. COERCIVITY

The level of de-magnetizing force it takes to degauss a tape or other magnetic storage medium.

20.3.5 COMPUTING ASSETS

Information of any kind processed by any means, including on personally owned hardware, using County information processing systems, networks, software, equipment, materials, or implements which are owned, managed, operated, maintained, or in the custody or proprietorship of the County or private entities. This includes, but is not limited to, Internet, Intranet, and Extranet applications, operating systems, network operating systems, storage media, network accounts, E-mail, file transfer protocol, documentation, and convergent devices such as the Personal Digital Assistant (PDA) and Smartphone.

20.3.6 COMPUTER FORENSICS

Computer forensics, also called cyber-forensics, is the application of computer investigation and analysis techniques to gather evidence suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computer and who was responsible for it.

20.3.7 DEGAUSS

To degauss is to de-magnetize. Degaussing a magnetic storage medium removes all the data stored on it. A degausser is a device used for this purpose.

20.3.8 DICTIONARY ATTACKS

A method used to break security systems, specifically password-based security systems, in which the attacker systematically tests all possible passwords beginning with words that have a higher possibility of being used, such as names and places, also trying the same passwords suffixed or prefixed with a numeric. The word “Dictionary” refers to the attacker exhausting all of the words in a dictionary in an attempt to discover the password. Dictionary attacks are typically done with software instead of an individual manually trying each password.

20.3.9 DIGITAL ARTIFACT

A piece of digital information, in whole or in part, generated by a computer's operating system and/or application program, which establishes that a specific activity has taken place.

20.3.10 DISASTER

A Disaster is any sudden, unplanned calamitous event that brings about significant damage or loss, creating an inability to support critical IT business functions for some predetermined period of time.

20.3.11 EXTRANET

An extranet is a private network that uses Internet protocols, network connectivity, and possibly the public telecommunication system to securely share part of an organization's information or operations with suppliers, vendors, partners, customers or other businesses.

20.3.12 FOBS

A small security hardware device with built in authentication often used to securely access a network. I20.3.13

INFORMATION SECURITY INCIDENT

An act of violating a County information technology security policy. This includes, but is not limited to: attempts (either failed or successful) to gain unauthorized access to a system or its data; unwanted disruption or denial of service; unauthorized use of a Computing Asset for the processing or storage of data; changes to a Computing Asset’s hardware, firmware, or software characteristics without the User’s knowledge, instruction, or consent. (See the Acceptable Use Policy.)

20.3.14 ITAC

County-wide Information Technology Advisory Committee maintains administrative governance over IT direction. It is intended to “serve as a forum to disseminate security-related information, promote awareness, and to create and recommend for adoption, County-wide IT security policies”.

20.3.15 ITSP

Information Technology Security Policy.

20.3.16 IT DISASTER RECOVERY

Defines the immediate short term processes needed to continue to offer critical IT services to clients. In a disaster situation, decreased services may be unavoidable.

20.3.17 ITST

Information Technology Security Team provides IT with a consistent security discipline, in cooperation with County departments.

20.3.18 MALWARE

For "malicious software", this is programming or files that are developed for the purpose of doing harm. Thus, Malware includes computer viruses, pervasive worms, Trojan horses, and the purposeful overloading of an E-mail account, etc.

20.3.19 MATTER

As defined in California Penal Code section 311 and 313, which can be found on the State of California, Office of Legislative Counsel’s Website: http://www.leginfo.ca.gov/calaw.html

20.3.20 NETWORK SNIFFING

Hardware and software normally used for monitoring and troubleshooting problems on the network. Used illegally, this technology would improperly obtain data, or slow the network response time.

20.3.21 PACKET SPOOFING

Packet Spoofing is when information being transmitted across the internet is changed to hide the read source of the data. This data is typically malicious in nature.

20.3.122 PATCH MANAGEMENT (PATCHES)

Patch management is an area of computer systems management that involves acquiring, testing, and installing multiple Patches (operating system or application software code changes) to an administered computer system.

20.3.23 PEER-TO-PEER

Peer-to-peer (referred to as P2P) is a type of transient network that allows a group of computer Users with the same networking program to connect with each other and directly access files from one another's hard drives.

20.3.24 PERSONAL DIGITAL ASSISTANT (PDA)

Personal digital assistants are versatile, handheld computers. PDAs are often referred to as pocket computers. PDAs gained popularity in the 1990s with the introduction of the Palm Pilot. Typical functionality includes a calculator, a clock and calendar, ability to play computer games, access to the Internet, sending and receiving E-mails, video recording, typewriting and word processing, use as an address book, making and writing on spreadsheets, use as a radio or stereo, and Global Positioning System (GPS). One of the most significant PDA characteristics is the presence of a touch screen.

20.3.25 PINGED FLOODS

Pinging is diagnostically used to ensure that a host computer, which you are trying to reach, actually operates. Used illegally, the Ping program would tie up the network by constantly Pinging a workstation or server.

20.3.256 PONZI SCHEME

Named after scam artist Charles Ponzi, who was famous for offering to "double your money in 90 days", early in the 20th century.

20.3.27 SMARTPHONE

A Smartphone is a specific type of a full-featured cellular (mobile) phone with personal computer like functionality. Smartphones are cellular phones that support full featured E-mail capabilities with the functionality of a complete personal organizer. In addition to the functionality of newer PDAs, features of most Smartphones include camera and video capabilities, removable memory or storage, applications such as E-mail, Microsoft Word, Microsoft Excel, and other enhanced data processing, the ability to connect to corporate (County) WAN/LANs for the uploading and downloading of data, a miniature keyboard, and a touch screen. Smartphones, when enabled with a cellular data plan, can access the Internet, intranets, or extranets.

20.3.28 SPAM

Spam is unsolicited E-mail on the Internet, generally equivalent to unsolicited phone marketing calls, except that the User pays for part of the message since everyone shares the cost of maintaining the Internet.

20.3.29 SPOOF

To deceive for the purpose of gaining access to someone else's resources. For example, to fake an Internet address so that one looks like a certain kind of Internet user.

20.3.30 THIRD-PARTY SERVICE ORGANIZATIONS

Any non-County organization that develops, installs, delivers, manages, monitors, or supports any County Computing Asset. These services may be rendered with a local physical connection, or via a variety of remote network connectivity options.

20.3.31 TROJAN HORSE

A Trojan horse is a malicious program that pretends to be a benign application. Trojans are not Viruses in the true definition as they do not replicate, but they can be just as destructive.

20.3.32 US-CERT

A partnership between the Department of Homeland Security's National Cyber Security Division (NCSD) and the private sector has been established to protect our nation's Internet infrastructure through global coordination of defense against, and response to, cyber incidents and attacks across the nation.

20.3.33 USENET NEWSGROUP

Usenet is a collection of User-submitted notes or messages on various subjects that are posted to servers on a world-wide network. Each subject collection of posted notes is known as a newsgroup.

20.3.34 USER

Any end User of County Computing Assets including: elected officials, full-time, part-time, and temporary County officers, agents, employees, contractors, consultants, and volunteers or any individual authorized to use County Computer

20.3.35 VIRUS

A Virus is a program or code capable of attaching to files and replicating itself repeatedly, and causing an unexpected, usually negative event. In practical terms, like the biological parasite, Viruses require a host computer pro- gram to survive, and generally infect an existing program on a computer and require user intervention to propagate.

20.3.36 WIPING

Wiping is essentially a software solution that provides the ability to destroy all data on a variety of data storage devices, preventing any possibility of future recovery of deleted files and folders.

20.3.37 WIRELESS ACCESS POINT

A station that transmits and receives data (sometimes referred to as a transceiver). An access point connects Users to other Users within the network and also can serve as the point of interconnection between the User and a fixed wire network.

20.3.28 WORM

Worms are computer programs that replicate over a network connection, but unlike Viruses, Worms exist as separate entities and do not infect other computer program files. Worms can spread themselves automatically via a net- work, and require no user intervention.

Computer Information Technology Security Program

"Acceptable User Policy Acknowledgement" Form

I have read and I understand my rights and obligations under this policy. I agree to comply with the policy. I understand that violation of this policy will likely result in serious Disciplinary Action up to and including dismissal.

SIGNATURE	
NAME	
TITLE	
DEPARTMENT	
DATE	

20.4 Enforcement

Any User of County Computing Assets, found to have violated this policy may be subject to appropriate disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil.

22 Preventing Theft of County-owned Hardware and Software

22.2 This policy applies to all County-owned hardware and software used by employees and visitors.

22.4.1.2 County equipment will be assigned to individual County staff and will be used exclusively by that staff unless permission is expressly granted by that employee's supervisor. Equipment is to be used for the purposes of performing County business and duties as outlined by the County of Tulare Information Technology Security Policy 2.0. and by the employee's supervisor. All equipment must be returned in proper working order in the event that an employee transitions from County employment or transfers to another Department within the County.

22.4.1.3 All County employees are responsible for the protection of County-owned assets. County employees are responsible for exercising reasonable effort to prevent any theft or damage that might occur within their work assignments.

22.4.1.3.1 Users must report the damage, loss or theft involving County-owned hardware and software to their supervisor immediately.

22.4.2 If there is evidence that a burglary or theft involving County-owned hardware or software has occurred, these additional requirements apply:

22.4.2.1 Notify the appropriate law enforcement agency (Sheriff or city police) and file an incident report.

22.4.2.2 Notify the TCiCT Service Desk via a written report or an email.

22.5.0 If appropriate County administrators conclude that an employee has engaged in theft involving County-owned hardware or software, appropriate disciplinary action will be taken, up to and including termination of employment, in accordance with applicable personnel policies.

23 Tulare County Mobile Device Policy

23.4.2.1 Employees using mobile devices and related software for network and data access will enroll in the county's Mobile Device Management system.

23.4.2.2 All mobile devices must be protected by a strong password. See TCiCT Security Password Policy 10 for additional details. Employees agree to never disclose their passwords to anyone.

23.4.2.2.1 Unless otherwise directed by the Department Head or required by business needs, the idle timeout must be set to a maximum of five minutes.

23.4.2.2.2 Unless otherwise directed by the Department Head or required by business needs, the grace period must be set to a maximum of one minute.

23.4.2.4 In the event of a lost or stolen mobile device, the user must report the loss to TCiCT immediately. The device will be remotely wiped of all data and locked to prevent access by anyone other than TCiCT. If the device is recovered, it can be submitted to TCiCT for re- provisioning.

23.4.5.1 Peer-to-Peer file-sharing applications will not be used on mobile devices to access County data.