INFORMATION TECHNOLOGY USAGE POLICY

COUNTY OF ORANGE

1 INTRODUCTION:

The County of Orange Information Technology (IT) Usage Policy is the foundation of the County's information security efforts. Each member of the County workforce is responsible for understanding his/her role in maintaining County IT security. This policy summarizes your information technology responsibilities. To learn more about information security, please see the Information Technology Security Policy.

Complete **Section 5: Acknowledgement** after you have finished reading this document. Your signature on the Acknowledgement indicates that you understand and will comply with County security policy. If you disregard security policies, standards, or procedures, you can be subject to County and agency-specific disciplinary action.

2 TERMS YOU NEED TO KNOW:

Authentication	The process of verifying the identity of anyone who wants to use County information before granting them access.
Back Up	To copy files to a second medium (for example, a disk or tape) as a precaution in case the first medium fails.
Confidentiality / Non-Disclosure Agreement	An agreement that outlines sensitive materials or knowledge that two or more parties wish to share with one another. By way of such agreement, the parties to the agreement agree not to share or discuss with outside parties the information covered by the agreement.
System or Software Configuration Files	Highly important files that control the operation of entire systems or software.
Electronic Communication	Messages sent and received electronically through any electronic text or voice transfer/storage system. This includes e-mail, text messages, instant messages (IM) and voicemail.
Encryption	The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to *decrypt* it. Unencrypted data is called *plain text*; encrypted data is referred to as *cipher text.*
Information Security	Safeguarding an organization's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.
Information Technology (IT)	The broad subject concerned with all aspects of managing and processing information within an organization.
Local Security Administrator (LSA)	The person at each agency who is responsible for the operational maintenance of IT security resources within the agency.
Network	Two or more linked computer systems. There are many different types of computer networks.
Password	Sequence of characters (letters, numbers, symbols) used in combination with a User ID to access a computer system or network. Passwords are used to authenticate the user before s/he gains access to the system.

Personally Identifiable Information (PII)	Any piece of information that could be used to uniquely identify, contact, or locate a single person. Examples include: full name; national identification number; email address; IP address; driver's license number; and Social Security Number.
User	Any individual who uses a computer.
User ID	Unique name given to a user for identification to a computer or telephone network, database, application, etc. Coupled with a password, it provides a minimal level of security.
Virus / Malicious Software	A software program that interferes with computer operation, damages or destroys electronic data, or spreads itself to other computers. Viruses and malicious software are often transmitted via email, documents attached to email, and the Internet.
Workforce Member	Any member of the County workforce, including employees, temporary help, contractors, vendors and volunteers.

3 POLICY OVERVIEW

As a member of the County workforce, you are expected to comply with the County's Information Technology Usage Policy. Your agency may have additional policies that you must follow as part of your job.

The following are key concepts of the County's policy:

- Information created or used in support of County business activities is the property of the County.
- Your assigned information technology resources are meant to facilitate the efficient and effective performance of your duties. It is your responsibility to ensure that resources are not misused and that you comply with policy.
- If you need to access confidential information as part of your duties, you will be asked to sign a confidentiality or non-disclosure agreement before you access the County network.
- Many County facilities house sensitive or critical information systems. You are expected to comply with all physical access controls designed to restrict unauthorized access.
- You may not remove County equipment or data in any format from the workplace unless you have received prior written approval from your supervisor or manager.
- The use of the network and Internet is a privilege, not a right. If you violate policy, you may lose your network and/or Internet access. The County may refuse to reinstate your access for the remainder of your employment at the County. The County may also take other disciplinary action as appropriate under County policy, departmental policy and applicable employment MOUs.

4 YOUR RESPONSIBILITIES

Your security responsibilities fall under several different Information Technology categories. Each category and the key responsibilities associated with it are listed below:

USER IDs AND PASSWORDS

- You will be issued a network user ID unique to you. Only you may use your user ID to access County resources (e.g. computer, telephone, FAX).
- You will be issued a default password at the same time as your user ID. You will be prompted to change your password the first time you log in to the system.
- Do not share user IDs and passwords with other users or individuals, including coworkers and supervisors. Treat your password as sensitive and highly confidential information.
- You are agreeing to follow the Information Technology Usage Policy when you accept a password from the County and use it to access the County data or telephone networks, the Internet, or the Intranet.
- Change your password immediately if you think someone else knows it. Report your suspicions to management.
- If you lose or forget your password, you are required to request a password reset. No one else can do it for you.

HARDWARE AND SOFTWARE

- The County will provide, and employees may request, peripheral equipment such as ear buds for cellular phones or Blackberry devices, as may be necessary to enable compliance with all local laws which pertain to the use of mobile communication equipment or the individual workplace needs for the employee to perform his or her employment.
- Never download or install any hardware or software without prior written approval of your agency IT representative.
- Do not make any changes to system and/or software configuration files unless specifically authorized in writing by your agency IT.
- Maintain your business data files on a network (or "shared") drive so that they can be backed up according to your agency's regular backup schedule.
- Use the "lock workstation" feature any time you leave your workstation logged on to the network and you are away from your desk.
- Do not connect a County laptop or other mobile device to the network until it has been scanned for viruses and malicious software.
- Follow the authentication procedures defined by your agency whenever you log in to the County network via Remote Access.
- Do not attempt to connect your workstation, laptop, or other computing device to the Internet via an unauthorized wireless or other connection while simultaneously connected to any County network.
- Retain original software installed on your computer if it is provided to you. The software must be available when your system is serviced in case it needs to be reinstalled.
- Do not keep liquids or magnets on or near computers, as they can cause serious damage.
- Ensure that your equipment is plugged into a surge protector at all times.

- Report all computer problems in detail on the appropriate form and/or when you contact the County Service Desk or discuss the problem with your agency's Help Desk.
- Report equipment damage immediately to the County Service Desk or your agency's Help Desk.

EMAIL and TELEPHONE

- The e-mail and telephone systems and networks are primarily for official County business.
- Management can freely inspect or review electronic mail and data files including voicemail. Employees should have no expectation of privacy regarding their internet usage, electronic mail or any other use of County computing or telephone equipment.
- Do not use a County email account or voicemail box assigned to another individual to send or receive messages unless you have been authorized, in writing, to act as that individual's delegate.
- Use of personal Internet (external) email systems from County networks and/or desktop devices is prohibited unless there is a compelling business reason for such use and prior written approval has been given by agency management and agency IT.
- Do not configure or use automated forwarding to send County email to Internet-based (external) email systems unless specifically authorized to do so, in writing, by County management.
- Send confidential information via email only with the written permission of management and only via an approved method. Mark the email according to agency policy.
- Treat confidential or restricted files sent as attachments to email messages as confidential or restricted documents. This also applies to confidential or restricted information embedded within an email message as message text or a voicemail message.
- Do not delete email or voicemail messages or other data if management has identified the subject matter as relevant to pending or anticipated litigation, personnel investigation, or other legal processes.

THE INTERNET / INTRANET

- Internet/Intranet access is primarily for County business.
- You may access the Internet for limited personal use only during nonworking time and in strict compliance with policy. If there is any doubt about whether an activity is appropriate, consult with your Department Head or his/her designee.

INFORMATION SECURITY

- Treat hardcopy or electronic Personally Identifiable Information (PII) as confidential and take all precautions necessary to ensure that it is not compromised. Intentional – or even accidental – disclosure of PII to unauthorized users is a violation of policy.
- Don't leave PII unattended or unsecured for any period of time.
- Be sure to follow your agency's policy for disposing of confidential data. This may include the physical destruction of data through shredding or other methods.
- Information created, sent, stored or received via the email system, network, Internet, telephones (including voicemail), fax or the Intranet is the property of the County.

- Do not expect information you create and store on County systems, including email messages or electronic files, to be private. Encrypting or using other measures to protect or "lock" an email message or an electronic file does not mean that the data are private.
- The County reserves the right to, at any time and without notice, access, read and review, monitor, and copy all messages and files on its computer system as it deems necessary.
- The County may disclose text or images to law enforcement without your consent as necessary.

PROHIBITED ACTIVITY

Unless you are specifically authorized by your manager or agency in writing, the following uses are prohibited by the Information Technology Security Policy:

- Using, transmitting, or seeking inappropriate or offensive materials, including but not limited to vulgar, profane, obscene, abusive, harassing, belligerent, threatening, or defamatory (harming another's reputation by lies) language or materials.
- Accessing, attempting to access, or encouraging others to access controversial or offensive materials.
- Revealing PII without permission, such as another's home address, telephone number, credit card number or Social Security Number.
- Making offensive or harassing statements or jokes about language, race, color, religion, national origin, veteran status, ancestry, disability, age, sex, or sexual orientation.
- Sending or soliciting sexually oriented messages, images, video or sound files.
- Visiting sites featuring pornography, terrorism, espionage, theft, drugs or other subjects that violate or encourage violation of the law.
- Gambling or engaging in any other activity in violation of local, state, or federal law.
- Uses or activities that violate the law or County policy or encourage others to violate the law or County policy. These include:
  - Accessing, transmitting, or seeking confidential information about clients or coworkers without proper authorization.
  - Intruding, or trying to intrude, into the folders, files, work, networks, or computers of others, or intercepting communications intended for others.
  - Knowingly downloading or transmitting confidential information without proper authorization.
- Uses that cause harm to others or damage to their property, including but not limited to:
  - Downloading or transmitting copyrighted materials without the permission of the copyright owner. Even if materials on the network or the Internet are not marked with the copyright symbol, ©, assume that they are protected under copyright law.
  - Using someone else's password to access the network or the Internet.
  - Impersonating another user or misleading message recipients into believing that someone other than the authenticated user is communicating a message.

- Uploading a virus, other harmful component, or corrupted data or vandalizing any part of the network.
- Creating, executing, forwarding, or introducing computer code designed to self-replicate, damage, or impede the performance of any computer's memory, storage, operating system, application software, or any other functionality.
- Engaging in activities that jeopardize the security of and access to the County network or other networks on the Internet.

- Downloading or using any software on the network other than that licensed or approved by the County.
- Conducting unauthorized business or commercial activities including, but not limited to:
  - Buying or selling anything over the Internet.
  - Soliciting or advertising the sale of any goods or services.
  - Unauthorized outside fund-raising activities, participation in any lobbying activity, or engaging in any prohibited partisan political activity.
  - Posting County, department and/or other public agency information to external news agencies, service bureaus, social networking sites, message boards, blogs or other forums.
- Uses that waste resources, including, but not limited to:
  - Printing of personal files.
  - Sending chain letters for any reason.
  - Including unnecessary recipients on an email. Only copy others on an email or voicemail message who should be "in the loop" on the topic addressed.
  - Indiscriminate use of distribution lists. Before using a distribution list, determine whether or not it is appropriate for everyone on that list to receive the email.
  - "All hands" emails. Emails of this type are to be sent only after management permission has been obtained.