INFORMATION TECHNOLOGY SECURITY POLICY

COUNTY OF IMPERIAL

1 INTRODUCTION

The County of Imperial Information & Technical Services (ITS) Security Policy is the foundation of the County's electronic information security efforts. Each member of the County workforce is responsible for understanding his/her role in maintaining County Information Technology security. This policy summarizes your information security responsibilities.

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. They 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.
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 department who is responsible for the operational maintenance of IT security resources within the department.
Network	Two or more linked computer systems.
Password	Sequence of characters (letters, numbers, symbols) used in combination with a User ID to access a computer system or network and to authenticate the user before *he/she* 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 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 GENERAL PRINCIPLES

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

- Information created or used in support of County business activities is the property of the County.
- Your assigned information technology resources are meant to help you perform your duties. It is your responsibility to ensure that resources are not misused.
- If you need to access confidential information as part of your duties, you may 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 from the workplace unless you have received appropriate prior approval.
- The use of the network and Internet is a privilege, not an entitlement. If you violate policy, you may lose your network and/or Internet access.

If you disregard security policies, standards, or procedures, you may be subject to discipline.

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.

• Do not share user IDs and passwords with other users or individuals, including coworkers and supervisors.

• Have your password changed immediately if you think someone else knows it. Report your suspicions to management.

• If you lose or forget your password, *you* will need to request a new password. No one else can do it for you.

HARDWARE AND SOFTWARE

• Before leaving your computer while logged on to the network, use the "Lock Computer" feature by pressing Ctrl-Alt-Delete.

• Never download or install any hardware or software without prior written approval from Department Head/Manager and/or ITS.

• It is prohibited to make any changes to system and/or software configuration files.

• Maintain your business data files on a network drive so that they can be backed up according to your department's regular backup schedule.

• Follow the authentication procedures defined by ITS 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.

• Do not keep liquids or magnets on or near computers, as they can cause serious damage.

• Ensure that all computer 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 Department's Help Desk.

• Immediately report equipment damage to ITS or your Department's Help Desk.

EMAIL

The email system and network are primarily for County business. Management is entitled to inspect or review electronic mail and data files.

• It is prohibited to use a County email account assigned to another individual to send or receive messages, i.e., to act as that individual's email delegate.

• Use of Internet (external) email systems from County networks and/or desktop devices is prohibited unless there is a business reason for such use.

• 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 ITS or management.

• 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.

• Do not delete email messages or other data if management has identified the subject matter as relevant to pending or anticipated litigation or other legal processes.

THE INTERNET / INTRANET

• Internet/Intranet access is primarily for County business.

INFORMATION SECURITY

• Treat hardcopy or electronic Personally Identifiable Information (PII) as confidential and take all precautions necessary to ensure that it is not compromised. Disclosure of PII to unauthorized users is a violation of this policy.

• Unless you are actively working with the data, PII must be kept secure.

• Be sure to follow your department's/ITS policy for disposing of confidential data. This may include the physical destruction of data through shredding or other methods.

• Information created, sent, or received via the email system, network, Internet, telephones or the Intranet is the property of the County subject to the "Confidentiality Restriction" below.

o 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.

o The County reserves the right to access, read and review, monitor, and copy all messages and files on its computer system as it deems necessary subject to the "Confidentiality Restriction" below.

o **PLEASE NOTE:** The County may be required under certain circumstances to disclose text or images to the appropriate agency without your consent subject to the "Confidentiality Restriction" below.

Confidentiality Restriction: When a need arises to access confidential computer files required by law to be maintained by any department, Information & Technical Services will access those files only through the respective department head to insure that all confidential material remains protected and confidential to the extent required by law.

PROHIBITED ACTIVITY

The following uses are prohibited:

• Using, transmitting, or seeking vulgar, profane, obscene, abusive, harassing, belligerent, threatening, or defamatory language or 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, illegal 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:

  o Accessing, transmitting, or seeking confidential information about clients or coworkers without proper authorization.

  o Intruding, or trying to intrude, into the folders, files, work, networks, or computers of others, or intercepting communications intended for others.

  o Knowingly downloading or transmitting confidential information without proper authorization.

• Uses that cause harm to others or damage to their property. These include:

  o 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.

  o Using someone else's password to access the network or the Internet.

  o Intentionally uploading a virus, other harmful component, or corrupted data or vandalizing any part of the network.

  o Creating, executing, forwarding, or introducing computer code designed to self-replicate, damage, or impede the performance of a computer's memory, storage, operating system, or application software.

  o Engaging in activities that jeopardize the security of and access to the County network or other networks on the Internet.

• Conducting unauthorized business or commercial activities including, but not limited to:

  o Buying or selling anything over the Internet.

  o Soliciting or advertising the sale of any goods or services.

  o Unauthorized outside fund-raising activities, participation in any lobbying activity, or engaging in any prohibited partisan political activity.

  o Posting County, department and/or other public agency information to external news agencies, service bureaus, social networking sites, message boards, blogs or other forums.

5 ACCEPTANCE

By signing this document, I acknowledge that I have read, understand and will comply with the County of Imperial Information & Technical Services Security Policy.

Workforce Member Name (please print): _____

Workforce Member Acceptance Signature: _____

Agency/Department: _____

Date: _____