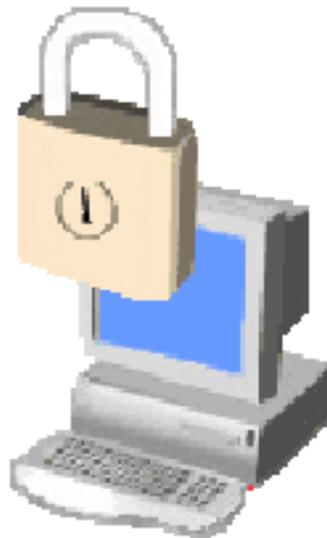


County of San Luis Obispo

Information Security Program



Information Security Policies

[MySLO>Employee Information>Information Security Program](#)

County-wide Information Security Policies

INFORMATION SECURITY PROGRAM:

MASTER SECURITY POLICY.....	4
ACCEPTABLE USE POLICY	7
ACCEPTABLE USE POLICY ACKNOWLEDGEMENT FORM.....	14
AWARENESS, TRAINING, AND EDUCATION POLICY	15
COMPUTER FORENSICS POLICY.....	18
INCIDENT RESPONSE POLICY	20
IT BUSINESS CONTINUITY PLANNING POLICY	23
IT WORKFORCE SECURITY POLICY	25
PASSWORD AND AUTHENTICATION POLICY	29
PATCH MANAGEMENT POLICY.....	33
PHYSICAL SECURITY POLICY.....	35
PORTABLE COMPUTING ASSET ENCRYPTION POLICY	37
PRIVACY AND CONFIDENTIALITY POLICY	39
REMOTE ACCESS POLICY.....	43
SECURITY LIFECYCLE AND AUDIT POLICY	47
SMARTPHONE - PDA POLICY.....	49
THIRD-PARTY IT SERVICE ORGANIZATIONS POLICY	52

VIRUS PROTECTION POLICY	54
WIRELESS COMMUNICATION POLICY	57
SECTIONS COMMON TO ALL POLICIES.....	58
OTHER AGENCY INVOLVEMENT.....	58
RELATED DOCUMENTS/POLICIES.....	58
ENFORCEMENT	59
DEFINITIONS	59

Countywide Information Security Program

Administrative Policy

Title: Information Security Program Master Security Policy

Effective Date: April 2, 2004
Prepared by: Countywide Information Security Committee
Review Date: September 4, 2010
Approved by: Information Technology Executive Steering Committee (IT-ESC)
Approval Date: September 4, 2009

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).

2. SCOPE

The County Information Security Program Master 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.

3. POLICY

3.1. Overview

3.1.1. 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:

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

- 3.1.1.2. Authentication – verify the identity of the sender and/or receiver of information.
 - 3.1.1.3. Data integrity – prevent unauthorized modification of systems and information.
 - 3.1.1.4. Availability – prevent disruption of service and productivity.
 - 3.1.1.5. Accountability – ensure correct use of the application and individual responsibility of that use.
 - 3.1.1.6. Audit ability – provide the ability to review/analyze logged security events both at the system and application software levels.
 - 3.1.1.7. Appropriate use – ensure Users conforms to County rules, ordinances and policy, and state and federal law.
- 3.2. Department heads, board members and elected officials (or their designee) responsibilities:
- 3.2.1. Ensures information security within their organization and adherence to countywide policies and procedures.
 - 3.2.2. Maintains any departmental information security policies.
 - 3.2.3. Coordinates a departmental information security incident response team. (see the ISP Incident Response Policy for more information)
- 3.3. User responsibilities:
- 3.3.1. Understands and adheres to County information security policies as well as appropriate organizational policies.
 - 3.3.2. Protects the County Computing Assets with which they are entrusted and uses them for their intended purposes.
 - 3.3.3. Signs an Acceptable Use Policy Acknowledgement as a condition of being granted access to County systems (see FORMS).
- 3.4. Information Technology Security Officer (ITSO) responsibilities:
- 3.4.1. Chair the countywide Information Security Committee.
 - 3.4.2. Provide information security related technical, regulatory, and policy leadership.
 - 3.4.3. Facilitate the implementation of County information security policies.
 - 3.4.4. Coordinate information security efforts across departmental lines.
 - 3.4.5. Lead continuing information security training and education efforts.

- 3.4.6. Serve as an information security resource to department heads and the Board of Supervisors.
- 3.4.7. Represent the County at professional information security forums and State and Federal events related to information security.

3.5. Countywide Information Security Committee responsibilities:

- 3.5.1. Provides a forum for Countywide information security-related collaboration and decision-making.
- 3.5.2. Strikes the balance of understanding the need for the County to continue operating its mission-critical applications, while simultaneously improving information security.
- 3.5.3. Develops, reviews, and recommends countywide information security policies to the IT Executive Steering Committee (IT-ESC), via the IT County Standards Committee (IT-CSC).
- 3.5.4. Develops, reviews, and recommends best practices, standards, guidelines and procedures to the IT-CSC.
- 3.5.5. Coordinates Inter-departmental communication and collaboration.
- 3.5.6. Coordinates departmental information security education and awareness.
- 3.5.7. May recommend appropriate hardware and software information security solutions.

4. FORMS

Acceptable Use Policy Acknowledgement, which is signed annually, either manually or electronically, by each User of County Computing Assets.

5. REVISION HISTORY

Version	Date	Chapter/Section	Details
1.4	Jan. 9, 2009	2.0	SCOPE: Added language re: not overridden by informal policies
1.3	June 1, 2007	3.1.1 2.0, 7.1	Add descriptors to the seven controls Add a reference to the full listing of security policies
1.2	May 5, 2006	3.2, 3.3, 4.3, 7	Removed all references to the DISR program and added ref. to Incident Response & Forensics Policies
		8	Removed "willfully" from the Enforcement Section
1.1	June 27, 2005	4.4 8.	Added "officers, agents" to USER definition (global change) "willfully" replaces "purposefully" in Enforcement section (global change)
1.0	April 2, 2004	All	New policy entitled <i>ISP Master Security Policy</i>

Countywide Information Security Program

Administrative Policy

Title: [Information Security Program Acceptable Use Policy](#)

Effective Date: April 2, 2004
Prepared by: Countywide Information Security Committee
Review Date: September 4, 2010
Approved by: Information Technology Executive Steering Committee
Approval Date: September 4, 2009

1. **PURPOSE**

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

2. **SCOPE**

This policy applies to all Users of County Computing Assets. Inappropriate use exposes the County to risks and threats to telecommunications, information systems, networks, facilities, and legal issues.

3. **POLICIES**

3.1. Overview

- 3.1.1. The County is committed to protecting itself from illegal or damaging actions, whether by intentional or unintentional means.
- 3.1.2. County Computing Assets are provided for conducting County business.
- 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 their activities in compliance with it.
- 3.1.4. A full listing of County Information Security Program Policies is listed under RELATED DOCUMENTS/POLICIES.

3.2. General Use and Ownership

- 3.2.1. The County may conduct audits or investigations on its Computing Assets to ensure compliance with this policy.

- 3.2.2. Nothing in this section will change the legal status of confidential or privileged information.
- 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.
- 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.
- 3.2.5. Authorized individuals within the County may monitor equipment, systems, and network traffic at any time for security, network maintenance and policy compliance purposes (see EXCEPTIONS).

3.3. Electronic Mail

- 3.3.1. County provided Internet E-mail sent to, or received from an Internet address, if undeliverable for a variety of reasons, may have its contents reviewed for the sole purpose of determining addressability.
- 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.
- 3.3.3. Message backup occurs by duplicating all messages and creating a storage copy. This procedure is performed nightly and held for a period of time. When authorized, messages can be restored from a backup copy. These procedures are intended for disaster recovery purposes, and not for customer convenience.
- 3.3.4. When establishing an E-mail 'out of office' agent, it is recommended that you do not automatically reply to E-mail from the Internet.

3.4. Instant Messaging

- 3.4.1. The use of Instant Messaging (IM) between County Users on County Computing Assets is permitted.
- 3.4.2. The use of Instant Messaging (IM) between County Users on County Computing Assets and any person on non-County Computing Assets is allowed only with Department Head approval.

- 3.4.3. IM is to be limited to text only. Attachments are not to be sent nor opened within IM.
 - 3.4.4. IM's are not to be used in circumstances where there is a policy or other requirement to preserve the communications.
 - 3.4.5. Final work products should be memorialized by accepted practices (i.e., letter or E-mail) not IM.
- 3.5. Use of County Provided E-mail, Internet services, access to commercial Instant Messaging, telephone services, and computers for Personal Use
- 3.5.1. The County provides E-mail, Internet services, access to commercial Instant Messaging, telephone services, and computers to enable Users to conduct the County's business in an efficient manner. These services and hardware systems are to be used in the direct conduct of the County's business.
 - 3.5.2. Except as otherwise stated, Users may occasionally use County provided Internet services, E-mail services, access to commercial Instant Messaging, telephone services, and computers for personal use. The User must limit their use so that the County's equipment is available for County use. The standard will be the same "reasonable use" standard that exists for use of County telephone equipment.
- 3.6. Security and Proprietary Information
- 3.6.1. 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 information, 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.
 - 3.6.2. All County Users must acknowledge 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:
 - 3.6.2.1.1. Are responsible for the security of their accounts.
 - 3.6.2.1.2. Are not authorized to share their passwords.
 - 3.6.2.1.3. Must change their password in accordance with individual application requirements.

3.6.3. Recommended Security Technologies

- 3.6.3.1. Password-protected screensavers, with automatic activation set at 10 minutes or less (of inactivity), are recommended on all PCs, laptops, and workstations.
 - 3.6.3.2. 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.
 - 3.6.3.3. 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.
 - 3.6.3.4. Use encryption, when/where available, for information that Users consider sensitive or vulnerable in compliance with established departmental standards.
- 3.6.4. Because information contained on portable computers is especially vulnerable, exercise special care in the handling, storage and transportation of this equipment.
- 3.6.5. 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.
- 3.6.6. Do not open E-mail attachments from an unknown sender, as it may contain malicious software, generally known as Malware (see DEFINITIONS).

3.7. Unacceptable Use

- 3.7.1. The following activities are prohibited. The three lists below are not exhaustive but attempt to provide a framework for activities that fall into the category of unacceptable use.

3.7.1.1. System Activities

- 3.7.1.1.1. Any purpose which violates applicable U.S., state, local laws, or County policies and their implementing regulations.

- 3.7.1.1.1.1. Using a County Computing Asset to knowingly engage in viewing, reading, creating, conveying, downloading, transferring, transmitting, scanning, or printing:

- 3.7.1.1.1.1.1. 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;

- 3.7.1.1.1.1.2. Any Matter in a manner that violates the San Luis Obispo County Policy Against Discriminatory Harassment;
- 3.7.1.1.1.1.3. Any illegal Matter (including child pornography) or sexually explicit images deemed by community standards to be obscene.
- 3.7.1.1.1.2. This provision does not apply to law enforcement and/or other County employees in situations where they are engaging in such activities in the performance of their job duties.
- 3.7.1.1.2. Using products that are not appropriately licensed for use by the County 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.
- 3.7.1.1.3. Abuse, damage, or exploitation of County Computing Assets.
- 3.7.1.1.4. 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 copyrighted software for which the County or the User does not have an active license.
- 3.7.1.1.5. 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.
- 3.7.1.1.6. 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.
- 3.7.1.1.7. Knowingly introducing Malware programs into any County Computing Asset.
- 3.7.1.1.8. Engaging in fraudulent offers of products, items, or services originating from any County Computing Asset.

3.7.1.2. Network Activities

- 3.7.1.2.1. 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.
- 3.7.1.2.2. 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.
- 3.7.1.2.3. Circumventing or mimicking (Spoofing) User authentication or security of any host, network, or account.
- 3.7.1.2.4. Interfering with or denying service to any Computing Asset other than the User’s own workstation (e.g., denial of service attack).
- 3.7.1.2.5. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable any Computing Asset, via any means, locally or via the Internet/Intranet/Extranet.
- 3.7.1.2.6. Providing information about, or lists of, County Users to parties outside the County, for other than authorized County business purposes.
- 3.7.1.2.7. 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.

3.7.1.3. E-mail and Communications Activities

- 3.7.1.3.1. 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).
- 3.7.1.3.2. Any form of harassment or discrimination via E-mail, telephone, or paging, whether through language, frequency, or size of messages.
- 3.7.1.3.3. 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>
- 3.7.1.3.4. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups, effectively producing newsgroup spam.

4. EXCEPTIONS

- 4.1. County electronic mail (E-mail) records may be accessed with written permission to the County GSA Director from the County Administrative Officer, or the User's department head.
- 4.2. A listing of Internet or Intranet sites visited by a User from a County Computing Asset may be requested with written permission to the County GSA Director from the County Administrative Officer, or the User's department head.
- 4.3. In response to subpoenas.
- 4.4. In response to Freedom of Information Act or California Public Records Act requests, only County information normally available to the public may be accessed.
- 4.5. Interdepartmental records requests must be approved in writing by the County Administrative Officer prior to submission to the County GSA Director.
- 4.6. Other access after consultation for legal review by County Counsel.

5. FORMS

ATTACHMENT: [Acceptable Use Policy Acknowledgement](#), which is signed annually by each authorized User of County Computing Assets.

6. REVISION HISTORY

Version	Date	Chapter/Section	Details
1.5	Sep. 4, 2009	3.4, 3.5	Added text regarding Instant Messaging
1.4	Jan. 9, 2009	Acknowledgement	Added a reference on the form to the mySLO location
1.3	June 1, 2007	3.1.4 and 8.5 3.6.1.1.1.1 and 4.4 3.6.1.3.2	Add a reference to the full listing of policies Changes that reflect "Matter" as the defining noun Add "or discrimination"
1.2	May 5, 2006	3.6.1.1.1	Added language prohibiting viewing, etc. obscene and illegal material
		9.0	Removed the word "purposely"
1.1	April 2, 2005	3.6.1.1.6	Added section: "Exporting, exploring, sharing or using for personal gain, data contained... This includes Users developing applications or accessing data for their own department or another County department."
1.1	April 2, 2005	4.2	Added "officers, agents"
1.0	April 2, 2004	All	New policy entitled <i>ISP Acceptable Use Policy</i>

COUNTY OF SAN LUIS OBISPO

Countywide Information Security Program

Computer Information Security Program

Acceptable Use Policy Acknowledgement Form

I acknowledge receipt of this policy and understand that I am bound by its contents:

SIGNATURE	
NAME	
TITLE	
DEPARTMENT	
DATE	

*The Acceptable Use Policy can be located on the County Intranet (mySLO):

[mySLO > Employee Information > Information Security Program > Policies](#)

Countywide Information Security Program

Administrative Policy

Title: [Information Security Program Awareness, Training, and Education Policy](#)

Effective Date: November 5, 2004
Prepared by: Countywide Information Security Committee
Review Date: September 4, 2010
Approved by: Information Technology Executive Steering Committee (IT-ESC)
Approval Date: September 4, 2009

1 PURPOSE

Information Security Awareness, Training, and Education (SATE) are keys to reducing the County's exposure to both malicious threats and accidental errors and omissions.

2 SCOPE

This policy applies to all Users of County Computing Assets. An increased level of SATE required for an individual employee may be determined by the department for that User's level of access to County Computing Assets.

3. POLICY

3.1. Overview

3.1.1. The term "Security Awareness" is considered the daily "moment-by-moment" awareness level, of these three fundamental principles:

- 3.1.1.1. CONFIDENTIALITY: Ensures that Users, including the public, only have clearance and access to the proper information.
- 3.1.1.2. INTEGRITY: Ensures that information cannot be modified, or destroyed, and is trusted.
- 3.1.1.3. AVAILABILITY: Ensures that information services are there when you need them.

3.2. Confidentiality

3.2.1. County data usually falls into two categories:

- 3.2.1.1. PUBLIC: At a minimum, all County public information must be reviewed by the department that 'owns' or 'controls' the information before it is released outside the department.
- 3.2.1.2. FOR OFFICIAL USE ONLY (FOUO): Includes, but is not limited to, personnel, medical, law and justice, and other sensitive, confidential, or privileged information.
- 3.2.2. See the Information Security Program Privacy and Confidentiality Policy for details regarding disposing of sensitive material and securing your workstation.
- 3.2.3. Secure access codes and other sensitive information, i.e., passwords, phone numbers.
- 3.2.4. Retrieve sensitive or confidential documents immediately from FAX, printers, and copy machines.

3.3. Integrity

- 3.3.1. It is every User's responsibility to protect the County's information that has been entrusted to them, and to ensure the authenticity of their work.
- 3.3.2. Be aware of people in your work area. Anyone not currently working in your unit or division may be considered a 'visitor', and not privy to certain information.
- 3.3.3. Do not: *
 - 3.3.3.1. Use a computer to harm other people
 - 3.3.3.2. Interfere with other User's computer work
 - 3.3.3.3. Look in other User's files unless authorized
 - 3.3.3.4. Use a computer to steal
 - 3.3.3.5. Pirate software
 - 3.3.3.6. Steal other's intellectual property
 - 3.3.3.7. Use a computer to pose as another User
 - 3.3.3.8. Use other User's Computing Assets without approval

* *Derived from the Computer Ethics Institute*

3.4. Availability

- 3.4.1. Maintain a secure backup, in another location, of your important computer files. These backups may minimize the loss of data if your Computing Asset experiences a failure.
- 3.4.2. Understand business continuity in your department, and its plans for operation in the event of a network, hardware, or software failure. (see the ISP IT Business Continuity Planning Policy and Framework)

3.5. Training and Education

- 3.5.1. GSA-IT will connect Users to current information and training aids by:
 - 3.5.1.1. Developing and distributing an annual training aid through new employee orientation and departmental workgroups.
 - 3.5.1.2. Broadcasting critical security bulletins to the County departmental automation staff.
 - 3.5.1.3. Publishing information security subjects and articles of interest on the County Intranet Web site.

4. REVISION HISTORY

Version	Date	Chapter/Section	Details
1.3	July 11, 2008	3.5.3 7.	Insert "critical" in front of "security bulletins" Update the Enforcement section changing "and/or legal penalties" to "legal action and/or penalties"
1.2	Oct. 30, 2006	None	Reviewed: No changes submitted
1.1	Jan. 23, 2006	4.2 7.0	Added "officers, agents" to User definition Removed "purposefully" from Enforcement
1.0	Nov. 5, 2004	All	New policy entitled <i>ISP Awareness Training and Education Policy</i>

Countywide Information Security Program

Administrative Policy

Title: [Information Security Program Computer Forensics Policy](#)

Effective Date: May 6, 2005
Prepared by: Countywide Information Security Committee
Review Date: September 4, 2010
Approved by: Information Technology Executive Steering Committee
Approval Date: September 4, 2009

1. PURPOSE

The purpose of this policy is to provide both education on the basic components of computer forensics, and describe how the County might cooperate with other agencies to fulfill a request for computer forensic service.

2. SCOPE

This policy applies to all Users of County Computing Assets.

3. POLICY

3.1. Overview

The objective of computer forensics is to provide valid and reproducible results when examining computer-related evidence. Computer forensics share all the legal and industry standard practice requirements of traditional forensic science. The methods used, and the results obtained by both may be presented in a legal setting in both adversarial and investigative proceedings.

3.2. Forensics Elements

- 3.2.1. Submissions may come from diverse sources and present unique examination issues.
- 3.2.2. Operating systems, which define what a computer is and how it works, vary among manufacturers. For example, forensic techniques developed for a personal computer using the Windows operating system will not correspond to that of Unix or Linux.
- 3.2.3. All application programs are unique and generate unique sets of Digital Artifacts.
- 3.2.4. Storage methods may be unique to both the device and the media.

3.3. Computer Evidence

- 3.3.1. Computer evidence is represented by physical items such as chips, boards, central processing units, storage media, monitors, and printers. Logging, describing, storage, and disposition of physical evidence are well understood by law enforcement, and authorized laboratories. They have detailed plans describing legal and acceptable methods for handling physical evidence.
- 3.3.2. Computer evidence is latent, and only stored in an electronic form on physical devices. The recovery of this latent information from the examination is then reported.
- 3.3.3. Computer evidence almost never exists in isolation. It is a product of the data stored, the application used to create and store it, and the computer system that directed these activities. To a lesser extent, it is also a product of the software tools used in the laboratory to extract it.

3.4. Handling Evidence

- 3.4.1. Digital evidence is extremely fragile. The chain of custody of digital evidence from computer user to forensic examiner must not be broken. Therefore, the first responder must not do anything to the computer and/or media involved that would cause the digital contents to be altered. County departmental computer technologists should not normally perform a forensics examination. Even unplugging a computer can alter evidence.
- 3.4.2. The department head or their designee should coordinate the decision to request forensic assistance, the securing of the area to be examined, and the handling of forensic evidence with specialists from other departments.
- 3.4.3. Generally, if a forensics request is initiated as a result of a personnel action, the first call should be to the Human Resources Department. All other forensic service requests should be directed to Information Technology, x2800.
- 3.4.4. County specialists securing the facility and assisting in forensics evidence gathering will most likely come from the following departments; Human Resources, County Counsel, Sheriff, General Services, Auditor Controller, and Information Technology.

4. REVISION HISTORY

Version	Date	Chapter/Section	Details
1.2	Jul 11, 2008	3.4.3, 3.4.4 7.0	Personnel to Human Resources Update the Enforcement section changing "and/or legal penalties" to "legal action and/or penalties"
1.1	Oct. 30, 2006	7.0	Removed "purposefully" from Enforcement
1.0	May 6, 2005	All	New policy entitled <i>ISP Computer Forensics Policy</i>

Countywide Information Security Program

Administrative Policy

Title: [Information Security Program Incident Response Policy](#)

Effective Date: November 5, 2004
Prepared by: Countywide Information Security Committee
Review Date: September 4, 2010
Approved by: Information Technology Executive Steering Committee (IT-ESC)
Approval Date: September 4, 2009

1. **PURPOSE**

This policy outlines the steps to be taken in the event of a real, perceived or potential Information Security Incident. To minimize Countywide impact, it is imperative that a formal reporting and response policy be followed when responding to Information Security Incidents.

2. **SCOPE**

This policy applies to all Users of County Computing Assets, whether or not on County premises.

3. **POLICY**

3.1. Overview

- 3.1.1. The intent of this policy is to define escalation points and individual roles in the event of an Information Security Incident. (see the ISP Acceptable Use, and Virus Protection Policies for more information)
- 3.1.2. Information Security Incidents generally originate in one of five categories:
 - 3.1.2.1. Malicious content, AKA Malware
 - 3.1.2.2. Users exploiting:
 - 3.1.2.2.1. Relaxed access control mechanisms resulting in damaged mission-critical information.
 - 3.1.2.2.2. Lack of auditing allowing altered data inputs and outputs from authorized applications.

- 3.1.2.3. Successful intrusions resulting in:
 - 3.1.2.3.1. Unauthorized access to information.
 - 3.1.2.3.2. A disruption or denial-of-service attack.
 - 3.1.2.3.3. Corruption or loss of information.
- 3.1.2.4. Theft or damage to Computing Assets.
- 3.1.2.5. Breach, violation, or misuse of County Information Security Policies.

3.2. Responsibilities

Designated personnel have the responsibility to take the action indicated in this section in a timely manner as dictated by the nature and severity of the incident. Those incidents having enterprise-wide implications should be given the most immediate attention, including escalation during any time period, 24hours/day, 7days/week.

3.2.1. Users

- 3.2.1.1. Report any perceived Information Security Incidents to your supervisor or manager.

3.2.2. Supervisor/Manager

- 3.2.2.1. Evaluate the reported Information Security Incident.
- 3.2.2.2. If within your purview, take initial action to isolate the incident.
- 3.2.2.3. Keep a record of actions taken.
- 3.2.2.4. If further action is required, notify GSA-IT Technical Support (x2800).
- 3.2.2.5. As necessary, notify the Sheriff's Office for assistance with theft of Computing Assets.
- 3.2.2.6. Refer to the ISP Computer Forensics Policy for computer evidence gathering and investigation.

3.2.3. Information Technology

- 3.2.3.1. Record and track the incident.
- 3.2.3.2. Route the incident to the GSA-IT Networking Section during working hours. After hours, the call will be routed to the GSA-IT manager on-call.
- 3.2.3.3. Recommend action and/or remediation as appropriate to:
 - 3.2.3.3.1. Reporting User/department
 - 3.2.3.3.2. GSA-IT staff
 - 3.2.3.3.3. Countywide automation staff mailing list

3.2.3.3.4. All County staff

4. REVISION HISTORY

Version	Date	Chapter/Section	Details
1.3	Jul 11, 2008	4.2 7.	Update definition of Security Incident, adding the word "County" in front of information security policy and adding a reference to the AUP. Update the Enforcement section changing "and/or legal penalties" to "legal action and/or penalties"
1.2	Jan. 29, 2007	3.1.1 6.1	Added reference to the AUP and Virus Protection Policies Added reference to the Virus Protection Policy
1.1	May 5, 2006	3.2.1, 3.2.2,4.2 3.2.2.6,6.1.3 4.4 7.0	Remove all reference to DISR Added ref. to the ISP Forensics Policy instead of Sheriff Added "officers, agents" Removed "purposefully" from Enforcement
1.0	Nov. 5, 2004	All	New policy entitled <i>ISP Incident Response Policy</i>

Countywide Information Security Program

Administrative Policy

Title: [Information Security Program IT Business Continuity Planning Policy](#)

Effective Date: May 6, 2005
Prepared by: Countywide Information Security Committee
Review Date: September 4, 2010
Approved by: Information Technology Executive Steering Committee
Approval Date: September 4, 2009

1. PURPOSE

Define the County's IT Business Continuity Planning (BCP) efforts and outline the process put in place to ensure the availability of essential IT systems and applications after a disaster.

2. SCOPE

This policy applies to all departments in the County.

3. POLICY

3.1 Overview

Regardless of an individual department's definition of a Disaster, an IT BCP is needed to meet an organization's IT security goals of *availability* of system resources, *integrity* for data and processes, and *confidentiality* of information.

Departments individually have the responsibility to develop and maintain an IT BCP based upon their need to maintain essential IT systems for the constituency of the County, other County departments, and outside agencies.

Current copies of a department's IT BCP and related data backups must be stored offsite at an alternate location(s) for use during a Disaster.

3.2 Outline the Plan

To adequately address IT BCP, at a minimum each department should have a documented plan that covers the following eight distinct phases. These eight phases are essentially the highest level from the table of contents in the Information Security Program IT Business Continuity Plan framework, available to each department.

- 3.2.1 IT Business Continuity Plan, Initiating and Housekeeping (Phase 1)
- 3.2.2 IT Business Impact and Risk Analysis (Phase 2)
- 3.2.3 Preparing for a Possible Emergency (Phase 3)
- 3.2.4 IT Disaster Recovery (Phase 4)
- 3.2.5 IT Business Recovery (Phase 5)
- 3.2.6 Testing the IT Business Recovery Process (Phase 6)
- 3.2.7 Training Staff in the IT Business Recovery Process (Phase 7)
- 3.2.8 Keeping the Plan Up-to-Date (Phase 8)

3.3. Maintaining the Plan

The IT BCP framework is designed as a flexible, up-to-date outline to assist departments with their plan definition efforts.

Given the need for the framework to be kept up-to-date, as well as the ongoing need for the completed departmental plans to be considered living documents, the IT Executive Steering Committee delegates the authority for maintenance of the IT BCP framework to the Information Security Committee.

4. REVISION HISTORY

Version	Date	Chapter/Section	Details
1.2	July 11, 2008	7.	Update the Enforcement section changing "and/or legal penalties" to "legal action and/or penalties"
1.1	Oct. 30, 2006	7.0	Removed "purposefully" from Enforcement
1.0	May 6, 2005	All	New policy entitled <i>ISP IT Business Continuity Planning Policy</i>

Countywide Information Security Program

Administrative Policy

Title: [Information Security Program IT Workforce Security Policy](#)

Effective Date: August 5, 2005
Prepared by: Countywide Information Security Committee
Review Date: September 4, 2010
Approved by: Information Technology Steering Committee
Approval Date: September 4, 2009

1. PURPOSE

The purpose of this policy is to outline IT related, pre- and post-employment requirements, as well as specific duties and responsibilities to safeguard the County and its workforce.

2. SCOPE

This policy applies to all Users of County Computing Assets and addresses several specific areas of IT security as it applies to the workforce including; employee background screening, termination/separation of County service, separation of IT duties and responsibilities, rotation of duties and responsibilities, and least privilege access to data.

3. POLICY

3.1. Background Screening

3.1.1. Background screening is a requirement placed on all prospective employees. (see the County Pre-Appointment Background Investigation and Drug Testing Policy maintained by the County Human Resources Department)

3.1.2. The original background screening and acknowledgement of the ISP Acceptable Use Policy must be completed before the Personnel “new hire paperwork” package is deemed complete.

3.2. Termination/Separation of County Service

3.2.1. When a User is terminating their relationship with the County, quick action is required to remove access to County Computing Assets by those no longer authorized to access those assets.

- 3.2.2. Any User being involuntarily terminated should be escorted from the premises upon notification to prevent further access to County Computing Assets. Voluntary terminations should be handled on a case-by-case basis at the discretion of the department head. (see the ISP Forensics Policy for related information)
 - 3.2.3. If the departing User has authority to grant access to, or is an administrator of departmental or enterprise County Computing Assets, this function should be re-assigned immediately. (see the ISP Password and Authentication Policy)
 - 3.2.4. Given that separations can occur regularly, County Computing assets should be protected through due diligence in the removal of access using the attached User Separation Checklist for County Computing Assets as a guide.
- 3.3. Separation of Duties and Responsibilities
- 3.3.1. An important element of operational security is the separation of duties and responsibilities, which is also known as a preventative control within information technology security. Staffing constraints within County departments may render some of the following recommendations either very challenging or impossible. In those cases, the value of departmental awareness and oversight of these roles and responsibilities cannot be overstated. Two main objectives exist in this control:
 - 3.3.1.1. That no one person acting alone can compromise the County's IT security. Said another way, collusion would need to be committed if the security practices were to be compromised.
 - 3.3.1.2. Mistakes are minimized in that no one person is performing all tasks from beginning to end within a project.
 - 3.3.2. The following are three examples of separation of duties and responsibilities:
 - 3.3.2.1. For individual workstations there must be a clear-cut line drawn between system administrator duties and end User duties. System administrators have the responsibility to assist with backup and recovery procedures, setting permissions, adding and removing Users, and developing User profiles. The end User on the other hand should have a secure environment to install programs, set passwords, alter desktop configurations, and modify certain system parameters.
 - 3.3.2.2. Jobs aligned with network hardware and software architecture should not be charged with, nor have access to, system administrator functions. Classic examples are the separation of staff charged with installation and maintenance of enterprise-wide systems such as E-mail and networking from the system administrator duties handling end User accounts.
 - 3.3.2.3. An application developer or vendor, moving a new or updated application to a production environment, should relinquish control to the appropriate operational function for installation, and should not

have routine access to production programs or data. This will have the added advantage of helping prevent mistakes, in that:

- 3.3.2.3.1. No one User is performing the end-to-end task,
- 3.3.2.3.2. Due diligence will have been performed to assure a complete product and clean hand-off.

3.4. Rotation of Duties and Responsibilities

- 3.4.1. The rotation of duties and responsibilities is an operational security control that ensures that multiple Users have knowledge and expertise to fulfill the obligation of more than one role or position.
- 3.4.2. This may seem juxtaposed to the Separation of Duties and Responsibilities section above. However, if fraud were attempted within a rotated position, it would be more easily detected by another User who knows how the tasks that should be performed in that position.
- 3.4.3. When viewed as a preventative security control, if User A knows that User B is going to replace them in that job function as it rotates, that knowledge alone may prevent a policy violation.

3.5. Least Privilege

Considered an administrative control, least privilege means that a User should have just enough permissions and rights to fulfill their role (business necessity.) If a User has excessive permissions and rights, it could open the door to abuse of access. (see the ISP Privacy and Confidentiality Policy)

4. FORMS

ATTACHMENT: User Separation Checklist for County Computing Assets

5. REVISION HISTORY

Version	Date	Chapter/Section	Details
1.2	July 11, 2008	7. Checklist	Update the Enforcement section changing "and/or legal penalties" to "legal action and/or penalties" Added FOBs
1.1	Oct. 30, 2006	8.0	Removed "willfully" from Enforcement
1.0	Aug. 5, 2005	All	New policy entitled <i>ISP IT Workforce Security Policy</i>

ATTACHMENT

User Separation Checklist for County Computing Assets:

General County Computing Assets

	Advise suppliers and vendors
	Badge
	Card keys
	Cell phone
	Computer and/or laptop
	County issued equipment/tools
	County-provided ISP accounts
	Departmental Manuals
	Dial-up access
	E-mail account
	FOBs
	Identification Card
	Keyless entry Account
	Keys (office, building, other)
	LAN print and file accounts
	Mailing lists
	Mainframe security
	Network access account
	Pager
	PDA
	Printer
	Purchasing card
	Telephone access
	Telephone calling card/account
	Voice mail
	VPN access
	Workstation login

Departmental Specific Computing Assets

Countywide Information Security Program

Administrative Policy

Title: [Information Security Program Password and Authentication Policy](#)

Effective Date: January 7, 2005
Prepared by: Countywide Information Security Committee
Review Date: September 4, 2010
Approved by: Information Technology Executive Steering Committee (IT-ESC)
Approval Date: September 4, 2009

1. PURPOSE

Establish a County standard for creation of strong passwords, the protection of those passwords, the frequency of change (AKA password aging), and define the current best practice for identification and authentication.

2. SCOPE

This policy applies to all Users of County Computing Assets.

3. POLICY

3.1. Overview

Passwords are an important aspect of computer security and are usually the front line of protection for User accounts. A poorly chosen password may result in the compromise of the County's entire enterprise network. As such, all Users are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Best practice for authentication to computer systems is moving from a simple User id and password, to a two-factor authentication scheme, discussed later in this document. While this is not the recommended County standard today, the County expects to monitor industry best practice implementation for applicability.

3.2. County Minimum User level Password Standard

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

3.3. General Password Protection

- 3.3.1.. All system-level passwords (e.g., servers, application administrators, security administrators) should be changed every 90 days.
- 3.3.2. System-level passwords (as listed in 3.3.1) shall be changed immediately upon the departure of an administrator from their assignment.
- 3.3.3.. All User-level passwords (e.g., E-mail, workstation, applications) shall be changed at least every 180 days. The interval should be shortened if you are unable to employ a complex password as set forth in section 3.2.
- 3.3.4. A good rule of thumb is the more important the data being secured, in conjunction with an increasing number of accesses, should drive the password aging to less days required before changing. The reverse should also hold true, up to the maximums listed above.
- 3.3.5. Passwords shall not be re-used once they have expired.
- 3.3.6. Passwords inserted into E-mail messages or other forms of electronic communication should be encrypted, and when possible they should be issued as single-use passwords.
- 3.3.7. Passwords shall not be written down unless stored in a locked safe for recovery purposes.

3.4. Strong Password Characteristics:

- 3.4.1. Contains six or more characters.
- 3.4.2. Contains both upper and lower case characters (e.g., a-z, A-Z).
- 3.4.3. Contain digits and punctuation characters as well as letters, (e.g., 0-9, ! # \$ % ^ & * () _ - + = \ : ; " ' { } [] < > , ? / .)

NOTE: not all systems allow for the use of mixed case and special characters.

- 3.4.4. Cannot be found in a dictionary.
- 3.4.5. Is not a common usage word such as the name of family member, pet, friend, co-worker, animated character, etc.
- 3.4.6. Doesn't use the word(s) "County", "San Luis Obispo", "SLO", County department name, or any derivation.
- 3.4.7. Doesn't contain birthdates or other personal information such as addresses, phone numbers, Social Security Numbers, or initials, or any part of the User name.

- 3.4.8. Doesn't use simple word or number patterns like aaabbb, zyxwvuts, 123321, etc., spelled forward or backward.
- 3.4.9. Is not any of the above preceded or followed by a digit.
- 3.5. Consider a Pass-Phrase
 - 3.5.1. Create a password based on a song title or other phrase, using the first character of each word. For example, the phrase might be: "One, Two, Three O'clock, Four O'clock Rock" and the password (pass-phrase) would then be something like "123Oc4OcR".
 - 3.5.2. All of the characteristics that make up a good password also apply to pass-phrases.
- 3.6. User Password Protection
 - 3.6.1 Do 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.)
 - 3.6.2. Never use the "Remember Password" feature of applications.
 - 3.6.3. Do not share County passwords with anyone, including administrative assistants, or family members.
 - 3.6.4. Do not share your password with co-workers while on vacation.
 - 3.6.5. If someone demands your password, refer them to this policy and your department head.
- 3.7. Application Development Standards
 - 3.7.1. Support identification and authentication for individuals, not groups.
 - 3.7.2. Attempt to authenticate to an existing, supported directory structure, failing that, at a minimum, make use of the adopted standard User id, and enforce this policy for password and authentication construction.
 - 3.7.3. Do not store passwords in clear text or in any easily reversible form.
 - 3.7.4. User passwords should not be available in clear text to system administrators.
 - 3.7.5. Do not store passwords within an application, this includes developer "backdoors".
- 3.8. Two-factor authentication is an evolving technology that has been adopted as the industry "Best Practice". It is evolving in the sense that the cost/benefit analysis doesn't yet regularly pan out as an agency standard for many outside the most secret of work sites. Two-factor authentication requires any two of the following:

- 3.8.1. Something you know: Password, pass-phrase, or PIN.
- 3.8.2. Something you have: Smart Card, access card, badge.
- 3.8.3. Something you are: Also called bio-metrics, these anatomical attributes are finger or thumb print, retina scan, palm scan, voiceprint, iris scan, etc.

4. REVISION HISTORY

Version	Date	Chapter/Section	Details
1.1	July 11, 2008	3.3.1 3.3.2 3.3.6 7.	Changed "shall" to "should" New section addressing a change in administrators requiring that when sending passwords via electronic communication they be encrypted and single use. Update the Enforcement section changing "and/or legal penalties" to "legal action and/or penalties"
1.1	Jan23, 2006	4.4 7.0	Added "officers, agents" Removed "purposefully" from Enforcement
1.0	Jan 7, 2005	All	New policy entitled <i>ISP Password and Authentication Policy</i>

Countywide Information Security Program

Administrative Policy

Title: [Information Security Program Patch Management Policy](#)

Effective Date: August 6, 2004
Prepared by: Countywide Information Security Committee
Review Date: September 4, 2010
Approved by: Information Technology Executive Steering Committee (IT-ESC)
Approval Date: September 4, 2009

1. PURPOSE

Computer Patch Management is a required discipline at the individual, departmental and enterprise levels to mitigate ongoing risks and threats to County Computing Assets.

2. SCOPE

This policy addresses the need for departmental Patch Management of Computing Assets under their control. Diligence within a department not only protects their investment, but in the case of self-propagating Malware, those Computing Assets Countywide.

3. POLICY

3.1. Overview

3.1.1. Updating of purchased software with vendor-supplied Patches is a required discipline to maintain correct functionality, and to protect the County's investment. Resources must be applied for assessment, preventative maintenance, and remediation.

3.2. Two disciplines should co-exist:

3.2.1. Pro-active preventative maintenance. Perform scheduled assessments identifying various threat levels including:

- 3.2.1.1. Operating system vendor announcements posted at the vendor site.
- 3.2.1.2. Anti-virus vendor updates and postings. (see the ISP Virus Protection Policy for more information)
- 3.2.1.3. Application vendor notifications and postings.
- 3.2.1.4. The [US-CERT](#) Web site containing Patches, bug-fixes, and workarounds considered noteworthy at the National level.

3.2.2. Re-active or responsive behavior to an announced, suspected, or actual threat:

3.2.2.1. The resources are the same as in the pro-active response, however, a sense of urgency is implied and some remediation might be required to keep or bring a Computing Asset back online.

4. EXCEPTIONS

Patch management on proprietary applications may require the vendor certification of Patches prior to application, inclusive of the underlying operating system.

9. REVISION HISTORY

Version	Date	Chapter/Section	Details
1.3	July 11, 2008	3.3 8.	Removed comment re: proactive vs. reactive Update the Enforcement section changing "and/or legal penalties" to "legal action and/or penalties"
1.2	October 30, 2006	8.0	Removed "willfully"
1.1	August 6, 2005	3.2.1.1 4.5 8.0	Removed vendor announcements from the ISP website Added "officers, agents" Changed "purposefully" to "willfully"
1.0	August 6, 2004	All	New policy entitled <i>ISP Patch Management Policy</i>

Countywide Information Security Program

Administrative Policy

Title: [Information Security Program Physical Security Policy](#)

Effective Date: June 3, 2005
Prepared by: Countywide Information Security Committee
Review Date: September 4, 2010
Approved by: Information Technology Executive Steering Committee
Approval Date: September 4, 2009

1. PURPOSE

The purpose of this policy is to outline the requirements for physical security of centralized and decentralized County Computing Assets.

2. SCOPE

This policy applies to all Users of County Computing Assets. Specifically, this policy is directed to the County data center and those shared, decentralized computing and network hosting facilities that have physical requirements greater than that of individual workstations. These facilities are locally known as; "Server Rooms", "Data Closets", "Networking Closets", or in some cases "Computer Rooms".

3. POLICY

3.1. Overview

The County requires that appropriate environmental, protective, and access control systems are in place to protect County Computing Assets housed in either the centralized County data center or within a decentralized facility.

3.2. Environmental Controls

Adequate environmental controls must be considered when locating significant Computing Assets. Heating, Ventilation, and Air Conditioning (HVAC), along with proper humidification and stable electrical power are considered the basics of environmental controls.

- 3.3. Protective Controls
 - 3.3.1 Identify and enforce physical security requirements.
 - 3.3.2. Use the tried and true policy of “least access”. Limit distribution and maintain records of access codes, cards, keys, fobs or combinations to those Users needing entry to fulfill their job requirements.
 - 3.3.3. Environmental, intrusion and fire alarm systems, and fire suppression systems may be considered for facilities hosting Computing Assets if the security risk warrants mitigation.
 - 3.3.4 Inventory and store data file backups and a current list of Computing Assets housed within these facilities at an off-site location per established retention schedules. (see the ISP IT Business Continuity Planning Policy)

- 3.4. Access Control Systems
 - 3.4.1. Maintain a current list of authorized service vendors allowed into the secure space.
 - 3.4.2. Identify and log any person accessing a secure space. Escort any person accessing a secure space wherein it is not part of their regular job requirements.
 - 3.4.3. Maintain stringent password security on enterprise level computing assets. (see the ISP Password and Authentication Policy)
 - 3.4.4. Report any suspected loss or theft of a Computing Asset to the appropriate management staff.
 - 3.4.5. Ensure proper disposal of a Computing Asset determined to be surplus, based upon departmental policy or applicable law. (see the ISP Privacy and Confidentiality Policy)

4. REVISION HISTORY

Version	Date	Chapter/Section	Details
1.2	Jul 11, 2008	7.	Update the Enforcement section changing “and/or legal penalties” to “legal action and/or penalties”
1.1	Oct. 30, 2006	3.3.2 7.0	Added “fobs” Removed “willfully”
1.0	June. 3, 2005	All	New policy entitled <i>ISP Physical Security Policy</i>

Countywide Information Security Program

Administrative Policy

Title: [Information Security Program Portable Computing Asset Encryption Policy](#)

Effective Date: September 4, 2009
Prepared by: Countywide Information Security Committee
Review Date: September 4, 2010
Approved by: Information Technology Executive Steering Committee (IT-ESC)
Approval Date: September 4, 2009

1. PURPOSE

To establish a policy regarding the protection of personal or confidential information used or maintained by the County that resides on any Portable Computing Asset.

2. SCOPE

This policy applies to all Users of County Computing Assets, whether or not on County premises who use Portable Computing Assets in support of County business.

3. POLICY

3.1. Overview

3.1.1. Placing personal or confidential information on Portable Computing Assets:

- 3.1.1.1. The County prohibits the unnecessary placement of Personally Identifiable Information (PII) or information classified as For Official Use Only (FOUO) on Portable Computing Assets.
- 3.1.1.2. Written authorization, signed by the department or agency head or their designee, must be granted prior to placing personal or confidential information on a Portable Computing Asset. This authorization must be reaffirmed annually at a minimum.
- 3.1.1.3. Every effort must be taken without limitation, to provide physical controls in order to protect personal or confidential information from unauthorized access and without exception, the information must be encrypted.
- 3.1.1.4. When it is determined that personal or confidential information must be placed on a Portable Computing Asset, every effort should be taken to minimize the amount of information required. If possible,

information should be abbreviated to limit exposure, e.g., the last four digits of the social security number.

- 3.1.1.5. In the event the Portable Computing Asset is lost or stolen, the department/agency must be able to recreate the personal or confidential information with 100 percent accuracy and must be able to provide notification to the persons/entities affected (see the ISP Privacy and Confidentiality Policy section DISCLOSURE: C.C. 1798.29(a).)
 - 3.1.1.6. Any actual or suspected loss or disclosure of personal or confidential information must be reported to the manager or department head responsible for the Portal Computing Asset (see the ISP Incident Response Policy.)
- 3.1.2. County minimum encryption requirements for Portable Computing Assets:
- 3.1.2.1. All County Portable Computing Assets containing personal or confidential information must at all times have automatic, full disk encryption that neither requires user intervention, nor allows the user a choice to implement.
 - 3.1.2.2. For the subclass of Portable Computing Assets that are considered portable storage media (see 4.2.3), they must be encrypted, whether they originate from a server, desktop workstation or portable computer.

4. REVISION HISTORY

Version	Date	Chapter/Section	Details
1.0	Sep. 4, 2009	All	New policy entitled <i>ISP Portable Computing Platform Encryption Policy</i>

Countywide Information Security Program

Administrative Policy

Title: [Information Security Program Privacy and Confidentiality Policy](#)

Effective Date: November 5, 2004
Prepared by: Countywide Information Security Committee
Review Date: January 9, 2010
Approved by: Information Technology Executive Steering Committee (IT-ESC)
Approval Date: January 9, 2009

1. PURPOSE

The dual purpose of this policy is to tie Privacy of individual's data to Information Security, and provide detailed examples applying Confidentiality to County Computing Assets.

2. SCOPE

This policy applies to all Users of County Computing Assets, whether or not on County premises.

3. POLICY

3.1. Overview

3.1.1. Maintaining Privacy requires that Users employ Confidentiality, thus the two subjects are inextricably linked when applied to information security.

3.1.2. PRIVACY generally protects information about individuals from unauthorized use, disclosure, or misuse of information.

3.1.3. CONFIDENTIALITY ensures that Users, including the public, only have clearance and access to the proper information.

3.2. Privacy

3.2.1. For the purposes of this policy as it relates to Information Technology, we will focus on the California Information Practices Act of 1977, found in Civil Code 1798, et seq. The following excerpts spell out the right to privacy and deal specifically with computerized data, its disclosure, and good faith acquisition.

3.2.1.1. THE LAW: C.C. 1798.1 “[T]he right to privacy is a personal and fundamental right as protected by Section 1 of Article I of the Constitution of California ...”

3.2.1.2. DISCLOSURE: C.C. 1798.29(a) “Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person ...”

3.2.1.3. PERSONAL INFORMATION: C.C. 1798.29(e) “For purposes of this section, ‘personal information’ means an individual’s first name or initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number. (2) Driver’s license number or California Identification Card Number. (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.”

3.2.1.4. GOOD FAITH : C.C. 1798.29(d) “[G]ood faith acquisition of personal information by an employee or agent of the agency for purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.”

3.2.2. There are many laws relating to privacy and confidentiality of personal information. All Users of County Computing Assets shall comply with laws relating to specific subject areas.

3.2.3. All County Users must acknowledge having received the County’s Acceptable Use Policy annually, to aid in individual awareness.

3.2.4. If authorized, appropriate E-mail and FAX disclaimers may be added to an outgoing correspondence (see ATTACHMENT). Your department will direct you in the use of a disclaimer, or for the need of a more specific disclaimer.

3.3. Confidentiality

3.3.1. County data usually falls into two categories:

3.3.1.1. PUBLIC: At a minimum, all County public information must be reviewed by the department that ‘owns’ or ‘controls’ the information before it is released outside the department.

- 3.3.1.2. FOR OFFICIAL USE ONLY (FOUO): Includes, but is not limited to, personnel, medical, law and justice, and other sensitive, confidential, or privileged information. Do not leave files or media containing FOUO information where an unauthorized person can see or obtain it. When not in use, FOUO information should be stored in a locked drawer or secure container.
- 3.3.2. Disposal of sensitive material:
 - 3.3.2.1. Printed material disposal is best accomplished by shredding. This can be accomplished locally or by a bonded vendor.
 - 3.3.2.2. Magnetic tape is most often re-used in a secure vaulting rotation throughout its lifecycle. Should the tape be deemed surplus, it should be Degaussed before being put to a new use. If no longer needed, the tape should be physically destroyed. It should be noted that today's modern tape has a high Coercivity specification. If there is any doubt that local "cleaning" methodologies fit the sensitivity of the data, destruction by a bonded vendor to ensure eradication is recommended.
 - 3.3.2.3. Fixed disks, diskettes, portable devices and removable drives that may be re-used should be 'Wiped'. The sophistication of 'Wiping' software ranges from shareware making a single pass writing data over all disk sectors, to the most sophisticated 7-pass, Department of Defense (DOD) approved software. Total destruction of fixed disks and diskettes can be accomplished by trained staff drilling several holes in the unit, or by disassembly of the disk with removal and destruction of the magnetic platter.
 - 3.3.2.4. CD/DVD media is easily destroyed by physically damaging the polycarbonate material. Cutting the disc in two with scissors or a paper cutter is the simplest office practice. DO NOT attempt to break this media with your hands by bending as injury may occur.
- 3.3.3. Suggestions for maintaining confidentiality at the workstation:
 - 3.3.3.1. Memorize your password(s) and remember you are responsible for everything done under your assigned User identification, do not share or write down this information.
 - 3.3.3.2. Take reasonable measures to ensure that your monitor is not in plain view of unauthorized persons.
 - 3.3.3.3. Shut down your computer when not in use for long periods of time.

4. REVISION HISTORY

Version	Date	Chapter/Section	Details
1.3	Jan. 9, 2009		No changes submitted
1.2	Jan 29, 2007		No changes submitted
1.1	Jan 23, 2006	4.5 7.0 Attachment	Added "officers, agents" Removed "purposely" from Enforcement New General non-disclosure statement provided by County Counsel
1.0	Nov 5, 2004	All	New policy entitled <i>ISP Privacy and Confidentiality Policy</i>

ATTACHMENT

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."

Countywide Information Security Program

Administrative Policy

Title: [Information Security Program Remote Access Policy](#)

Effective Date: August 6, 2004
Prepared by: Countywide Information Security Committee
Review Date: July 11, 2009
Approved by: Information Technology Executive Steering Committee
Approval Date: July 11, 2008

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 (WAN/LAN).

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.

3. POLICY

3.1. Overview

- 3.1.1. All remote access to the County WAN will be accomplished via a secure method, i.e., strong authentication and encryption.
- 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 ISP Privacy and Confidentiality Policy for more information)
- 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.
- 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. Interdepartmental transferees will only have their department-specific resources terminated.

3.2. Use and Awareness

- 3.2.1. See the Countywide Information Security Program Acceptable Use Policy for details regarding authorized use, personal use, security, unacceptable use, and monitoring. Remote access is considered a privilege, and can be revoked at any time without cause by the authorizing department head.
- 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.
- 3.2.3. Remote sessions that are inactive for more than 30 minutes may be discontinued automatically.
- 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 (sample attached).
- 3.2.5. Users accessing the County via remote-control applications such as PC Anywhere, VNC, MS Windows Remote Desktop, etc., must do so with software issued by their department, and with the full knowledge of their department.
- 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 serviceable 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.
- 3.2.7. Three unsuccessful attempts to sign on to the remote facility due to an incorrect userid or password may result in the temporary revocation of the account. Users must call GSA-IT to have their logon reset.
- 3.2.8. Application forms and instructions for remote access are available from Information Technology.

5. FORMS

ATTACHMENT: Authorization for Removal of County Equipment (SAMPLE)

6. REVISION HISTORY

Version	Date	Chapter/Section	Details
1.3	July 11, 2008	1. 7.	Clean up WAN/LAN language under Purpose to match that in the Wireless Policy Update the Enforcement section changing "and/or legal penalties" to "legal action and/or penalties"

1.2	October 30, 2006	3.2.5 8.0	Added "MS Windows Remote Desktop" Removed "willfully"
1.1	August 6, 2005	3.1.2 4.2 8.0	Replaced "sensitive or restricted" with FOUO Added "officers, agents" Changed "purposefully" to "willfully"
1.0	August 6, 2004	All	New policy entitled <i>ISP Remote Access Policy</i>

ATTACHMENT

(SAMPLE)

TO: All Concerned Parties

FROM: _____, (department head)

DATE: _____

SUBJECT: **Authorization for Removal of County Computing Assets**

This notice authorizes the following County User to remove the Computing Assets designated below from County premises, for the purpose of conducting County business:

User: _____ User #: _____

Item: _____ Serial No: _____

This equipment will be returned to County premises by (circle all that apply):

- a. The following date _____ / _____ / _____
- b. The need for replacement
- c. The User's termination date

User's signature: _____

User's name (printed): _____

Authorizing signature: _____

Countywide Information Security Program

Administrative Policy

Title: Information Security Program Security Lifecycle and Audit Policy

Effective Date: June 3, 2005
Prepared by: Countywide Information Security Committee
Review Date: July 11, 2009
Approved by: Information Technology Executive Steering Committee
Approval Date: July 11 2008

1. PURPOSE

The purpose of this policy is to ensure that County Computing Assets are properly designed and implemented to meet County information security requirements, and that appropriate audit controls are considered.

2. SCOPE

This policy applies to all County Computing Assets and relates to three broad layers of information technology product security; Administrative, Physical and Technical.

3. POLICY

3.1. Overview

3.1.1 Administrative Security comes into play primarily in policy, procedures, standards, workforce controls, and audits.

3.1.2. Physical Security relates to the environment, personnel safety, facility planning, alarms, and access systems.

3.1.3. Technical Security is generally software-based and enterprise architecture directed.

3.2. Lifecycle Requirements

3.2.1. Security requirements should be explicitly detailed in the project management component of all information technology initiatives during the project initiation phase.

3.2.2. At each phase of a product's development lifecycle, security requirements must be addressed for compliance with the County's enterprise architecture framework.

3.3. Audit Requirements

- 3.3.1. Computing Assets should be developed and/or implemented with the ability to capture and record various kinds of system activities such as operating system activity, application events, and User actions – the higher the level of security needed, the more activities should be captured. This data is also called an “activity” or “event” log which provides auditing capabilities.
- 3.3.2. Security audits should be conducted to ensure both compliance with County policy and the confidentiality, integrity and availability of County Computing Assets. Audits can be useful to verify the health of a system and provide accountability by detecting intrusions, reconstructing events, verifying that security policies are enforced, and producing summary reports. (see the ISP Acceptable Use Policy section 3.2)
- 3.3.3 Activity logs are normally reviewed two ways:
 - 3.3.3.1. Manual reviews which are normally event-oriented, or event-triggered.
 - 3.3.3.2 Automated tools can perform real-time analysis of audit trail information to detect anomalies, verify the baseline security and monitor the overall health of a Computing Asset.

4. REVISION HISTORY

Version	Date	Chapter/Section	Details
1.2	July 11, 2008	7.	Update the Enforcement section changing “and/or legal penalties” to “legal action and/or penalties”
1.1	Oct. 30, 2006	7.0	Removed “willfully”
1.0	June. 3, 2005	All	New policy entitled <i>ISP Security Lifecycle and Audit Policy</i>

Countywide Information Security Program

Administrative Policy

Title: Information Security Program Smartphone - PDA Policy

Effective Date: June 1, 2007
Prepared by: Countywide Information Security Committee
Review Date: January 9, 2010
Approved by: Information Technology Executive Steering Committee
Approval Date: January 9, 2009

1. PURPOSE

The purpose of this policy is to define the minimum security standards for connecting Smartphones and Personal Digital Assistants (PDAs) to the County Network (WAN/LAN).

2. SCOPE

This policy applies to all Users of County Computing Assets who intend to connect a personal or County-owned Smartphone or PDA to the County WAN/LAN or other County Computing Asset. Smartphones and PDAs are also known as “convergent devices”.

3. POLICY

3.1. Overview

This policy will define the acceptable security standards for connectivity of Smartphone and PDA devices. Note: This policy does NOT supersede any applicable HIPAA policies or other legal regulations that may apply to County Computing Assets.

3.2. Acceptable Uses

Connecting Smartphones and PDAs to the County WAN/LAN is acceptable provided the hardware and software standards set by the County Standards Committee (CSC) are followed. Adopted standards can be found on the County of SLO Bulletin Board, under County Standards Committee. These standards define the appropriate equipment types and minimum security ratings for devices connected to the WAN/LAN or other County Computing Assets (see related Smartphone Recommendations for standards.)

- 3.3. Connectivity
 - Connectivity of Smartphone or PDA devices comes in two forms: wired and wireless. In both cases, once a connection is established, data is transferred between the device and County Computing Assets. Connectivity must be via an approved County enterprise standard.
 - 3.3.1. Wired connectivity involves the physical connection of the device to a County Computing Asset such as a Personal Computer (PC). In this configuration, a wire is connected to both the Smartphone or PDA and the PC.
 - 3.3.2. Wireless connectivity can occur directly via an Infrared port to a County Computing Asset or via a cellular telephone data connection.
 - 3.3.3. When connecting a Smartphone or PDA device to the County network via a wireless cellular network, or other network not managed by the County, there is a possibility that some of the connections may not be secure as the data moves between vendors.
- 3.4. Passwords
 - Smartphone or PDA devices used to connect to County Computing Assets must be configured with a password to access and/or use information on the device. If the device remains active and is not manually locked, the device should automatically lock the user out of the keyboard requiring them to re-enter a password to access data on the device.
- 3.5. Encryption
 - All data transmitted to a Smartphone or PDA device over the air (OTA) via a County Computing Asset should be encrypted end-to-end with at least 128-bit SSL encryption. Users of these devices should ensure that their device is designed and configured to use 128-bit SSL encryption by default prior to making a purchase.
- 3.6. Virus Protection
 - Smartphone or PDA devices used to connect or synchronize to County Computing Assets should be protected by approved virus protection software. Virus protection products should be updated on a regular basis.
- 3.7. Responsibilities
 - 3.7.1. Lost or stolen Smartphone or PDA devices, used to access County functions or data, whether personally or County-owned must be reported immediately to your supervisor or manager (see the ISP Privacy and Confidentiality Policy regarding the law and protection of certain data.)
 - 3.7.2. The County assumes no responsibility for damage to personal Smartphones or PDA devices used to conduct County business. This pertains to physical damage as well as to “damaged” software. Given their potentially high replacement cost, the County recommends that individuals consider the purchase of insurance, at their sole cost, to cover the costs of a damaged phone.
 - 3.7.3. When disposing of damaged or outdated Smartphones or PDA devices, software tools should be used to ensure that residual data is removed. If the device memory cannot be erased, the device should be destroyed. If taking this path, remember to recycle the Li-Ion battery first.

4. REVISION HISTORY

Version	Date	Chapter/Section	Details
1.1	Jan. 9, 2009		No changes submitted
1.0	June 1, 2007	All	New policy entitled <i>Smartphone - PDA Policy</i>

Countywide Information Security Program

Administrative Policy

Title: [Information Security Program Third-Party IT Service Organizations Policy](#)

Effective Date: May 6, 2005
Prepared by: Countywide Information Security Committee
Review Date: July 11, 2009
Approved by: Information Technology Executive Steering Committee
Approval Date: July 11, 2008

1. PURPOSE

This policy describes the information security requirements for Third-Party IT Service Organizations that are engaged by the County.

2. SCOPE

This policy applies to any use of Third-Party IT Service Organizations by any County department.

3. POLICY

3.1. Overview

The project-sponsoring department within the County has the responsibility for compliance with this policy by the Third-Party IT Service Organization. An IT security risk assessment should be performed prior to commencement of work, and in cooperation with GSA-IT (as necessary) to determine what, if any security controls should be implemented to protect the County's Computing Assets.

3.2. Third-Party IT Service Organization Requirements

3.2.1. Agree to share their IT security policies and controls that will be used to protect the County's Computing Assets.

3.2.2. Submit to County audits, and independent audits sponsored by the County, performed to ensure compliance with County policies and proper security controls.

3.2.3. Sign the form acknowledging receipt of the Information Security Program (ISP) Acceptable Use Policy. This applies to each member of the Third-Party IT Service Organization who will provide services to the County.

3.2.4. Ensure that any computer systems attached to County Computing Assets will be in compliance with the ISP Patch Management and Virus Protection Policies.

3.2.5. Ensure compliancy with the County's ISP Remote Access Policy if accessing County Computing Assets remotely.

4. REVISION HISTORY

Version	Date	Chapter/Section	Details
1.2	Jul 11, 2008	7.	Update the Enforcement section changing "and/or legal penalties" to "legal action and/or penalties"
1.1	Oct. 30, 2006	7.0	Removed "purposely"
1.0	May 6, 2005	All	New policy entitled <i>ISP Third Party IT Service Organization Policy</i>

Countywide Information Security Program

Administrative Policy

Title: [Information Security Program Virus Protection Policy](#)

Effective Date: August 6, 2004
Prepared by: Countywide Information Security Committee
Review Date: January 9, 2010
Approved by: Information Technology Executive Steering Committee (IT-ESC)
Approval Date: January 9, 2009

1. PURPOSE

Virus protection software must be installed and kept current on all applicable County Computing Assets to prevent the harmful effects of Malware (see definitions).

2. SCOPE

This policy applies to all Users of County Computing Assets. Viruses and other Malware often have an impact Countywide and are not just limited to a single infected computer. In a networked environment, the weakest link in the chain can breach the security of the entire network.

3. POLICY

3.1. Overview

3.1.1 The intent of the policy is to generally define roles and responsibilities as they apply to protecting County Computing Assets from Malware distributed in the form of a computer Virus.

3.2 User Responsibilities

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

3.2.2. Be selective when downloading or receiving information and files from the Internet.

3.2.3. Keep personal use to a minimum to further reduce the possibility of receiving Virus-infected files. Parameters are established in the Information Security Program Acceptable Use Policy.

- 3.2.4 Report suspected Virus infection incidents to your supervisor or manager, departmental automation staff, and GSA-IT Technical Support, (see the ISP Incident Response Policy)
- 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 Security Program Remote Access Policy for more information.
- 3.2.6. Vendor workstations and servers, connected to County Computing Assets, are subject to the same Virus protection requirements as those owned by the County (see User definition). The responsibility for compliance rests with the department contracting with the vendor. (see the ISP Third Party IT Service Organizations Policy for more information)

3.3 Departmental Responsibilities

- 3.3.1 Ensure that all County Computing Assets have current Virus protection software installed.
- 3.3.2 Ensure that Virus protection pattern files and scan engines are updated automatically.
- 3.3.3 Ensure that workstation Virus protection software and related tools are installed and configured only by knowledgeable departmental or GSA-IT personnel.
- 3.3.4 Coordinate Virus protection updates with operating system patches as necessary. See the Information Security Program Patch Management Policy for more information.

3.4 GSA-IT Responsibilities

- 3.4.1 Work with appropriate staff to ensure that current enterprise Virus protection software and related tools are available Countywide.
- 3.4.2 Proactively notify the Countywide automation contact list of high-risk Viruses, preventative actions and remediation, as soon as they are known to be in circulation within the County's network, or pose a risk to mission critical applications.
- 3.4.3 Architect and monitor the overall design, function, and effectiveness of the Virus protection systems used throughout the County.

4. EXCEPTIONS

Certain proprietary application vendors recommend against the installation of virus protection, since the scanning software may interfere with certain application processes and database structures. These exceptions should be mitigated by other forms of protection and approved in advance by the department head in writing (E-mail O.K.).

7. REVISION HISTORY

Version	Date	Chapter/Section	Details
1.4	Jan. 9, 2009	4	Add department head approval in Exceptions
1.3	July 11, 2008	3.2 8.	Expand attachments past E-mail to I.M. and Internet downloads. Update the Enforcement section changing "and/or legal penalties" to "legal action and/or penalties"
1.2	Jan. 29, 2007	3.2.4 7.0	Added "supervisor or manager" Added "Incident Response Policy"
1.1	August 6, 2005	3.4.2 4.4 8.0	Combined 3.4.2 & 3.4.3 concerning notification Added "officers, agents" Changed "purposefully" to "willfully"
1.0	August 6, 2004	All	New policy entitled <i>ISP Virus Protection Policy</i>

Countywide Information Security Program

Administrative Policy

Title: [Information Security Program Wireless Communication Policy](#)

Effective Date: May 6, 2005
Prepared by: Countywide Information Security Committee
Review Date: January 9, 2010
Approved by: Information Technology Executive Steering Committee
Approval Date: January 9, 2009

1. PURPOSE

The purpose of this policy is to define the minimum engineering and security standards for connectivity to the County Wide Area Network / Local Area Network (WAN/LAN).

2. SCOPE

This policy applies to all Users of County Computing Assets who intend to establish a Wireless Access Point that is connected to the County WAN/LAN.

3. POLICY

3.1 Overview

This policy will define the acceptable engineering and security standards for wireless computer communication, and define the appropriate uses of this technology for direct connection to the County WAN/LAN.

3.2 Minimum Standard

The current minimum standard for hardware/software approved for use by the County, as developed by the Institute of Electrical and Electronics Engineers (IEEE), are 802.11i capable devices with 802.1x authentication.

3.3 Acceptable Uses

Wireless LAN (WLAN) connectivity to the County WAN/LAN is an acceptable use of Computing Assets provided the hardware and software standards set by the County Standards Committee (CSC) are followed. These standards define the appropriate equipment types and minimum security ratings for devices connected to the WAN/LAN.

4. REVISION HISTORY

Version	Date	Chapter/Section	Details
1.3	Jann 9, 2009	1.	Aligned the Purpose statement with that in the Remote Access Policy
1.2	Jan. 29, 2007		No Changes Submitted
1.1	Jan. 23, 2006	3.x 4.2 4.3 7.0	Modification to make wireless use acceptable based upon CSC recommended standards. Added "officers, agents" Added a definition for Wireless Access Point, removed the War Driving definition. Removed "purposefully" from Enforcement
1.0	May 6, 2005	All	New policy entitled <i>ISP Wireless Communication Policy</i>

SECTIONS COMMON TO ALL POLICIES

OTHER AGENCY INVOLVEMENT

Information Technology will work cooperatively with all County departments, outside governmental agencies, and vendors performing information technology work with the County, to ensure safe and secure information systems, as well as to protect the core enterprise architecture.

RELATED DOCUMENTS/POLICIES

Information Security Program policies in effect:

- Acceptable Use Policy (acknowledgement form attached)
- Awareness, Training and Education Policy
- Computer Forensics Policy
- Incident Response Policy
- IT Business Continuity Policy and Framework
- IT Workforce Security Policy
- Master Security Policy
- Password and Authentication Policy
- Patch Management Policy
- Physical Security Policy
- Portable Computing Asset Encryption Policy
- Privacy and Confidentiality Policy
- Remote Access Policy

Security Lifecycle and Audit Policy
Smartphone-PDA Policy
Third Party IT Service Organizations Policy
Virus Protection Policy
Wireless Communication Policy

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.

DEFINITIONS

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, deliberate, 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.

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.

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.

COUNTYWIDE INFORMATION SECURITY COMMITTEE (I-SEC)

“To serve as a forum to disseminate security-related information, promote awareness, and to create and recommend for adoption, Countywide IT security policies to the Executive Steering Committee, via the County Standards Committee” (as defined in the I-SEC charter).

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.

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.

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.

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.

DISR

Department Information Security Representative(s) provide oversight for the information security practices within a department, and may represent the department on the Countywide Information Security Committee on a rotating basis.

INFORMATION SECURITY INCIDENT

Is the act of violating a County information 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)

INSTANT MESSAGING

Instant messaging (sometimes call IM or IMing) is the ability to easily see whether a co-worker is connected to the network and, if they are, to exchange informal messages with them. Instant messaging differs from ordinary E-mail in the immediacy of the message exchange, and also makes a continued exchange quicker than sending E-mail back and forth.

IT-CSC

County Standards Committee, subordinate to the IT-ESC, charged with reviewing and recommending countywide IT standards.

IT-ESC

Countywide Information Technology Executive Steering Committee maintains administrative governance over IT direction.

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.

ITSO

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

MALWARE

For "malicious software", 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.

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>

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.

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.

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 characteristic is the presence of a touch screen.

PERSONALLY IDENTIFIABLE INFORMATION (PII)

The following is a representative list of individual pieces information that when used alone or in combination may lead to the identification of a specific person:

- Names
- All geographic subdivisions smaller than a state, including street addresses, city, county precinct, zip codes
- All elements of dates related to an individual, including birth date, admission or discharge date, date of death
- Medical record numbers
- Telephone and FAX numbers
- Driver license number
- E-mail addresses
- Social Security numbers
- Health plan beneficiary numbers

- Account numbers
- Certificate/license numbers
- Vehicle identifiers, serial numbers, license plate numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number or characteristics

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.

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.

PORTABLE COMPUTING ASSET

The following is a representative list of qualified Portable Computing Asset devices:

- Portable computers such as laptops, netbooks and tablet computers
- Portable devices capable of storing data such as personal digital assistants (PDA), portable phones, pagers, and digital cameras
- Portable storage media such as diskettes, tapes, CDs, zip disks, DVDs, flash memory/drives, and USB drives

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.

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.

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.

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.

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.

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.

USENET NEWSGROUP

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

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 Computing Assets.

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 program to survive, and generally infect an existing program on a computer and require user intervention to propagate.

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.

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.

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 network, and require no user intervention.

REVISION HISTORY FOR COMMON SECTIONS

Version	Date	Chapter/Section	Details
1.1	Sep. 4, 2009	Definitions All	Added definitions for Personally Identifiable Information, Instant Messaging & Portable Computing Asset. Changed all "ITD" to "GSA-IT" and Chief Information Officer to GSA Director (entire document).
1.0	Jan. 9, 2009	All	Created a compiled version of the policies and moved the common sections, including definitions to the end of the document. Previous changes to the common sections are noted within each policy. COMPUTING ASSET: Added Personally Owned, and Convergent Devices. And SMARTPHONE, replaced E-mail Bombs with, "the purposeful overloading of an E-mail account." OTHER AGENCY INVOLVEMENT: Slight language cleanup by Co. Counsel