COUNTY OF SAN LUIS OBISPO

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: April 8, 2012
Approved by: Information Technology Executive Steering Committee (IT-ESC)
Approval Date: April 8, 2011

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 provide:

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 the Acceptable Use Policy Acknowledgement form 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 *ISP Master Security Policy*

COUNTY OF SAN LUIS OBISPO

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: November 4, 2012
Approved by: Information Technology Executive Steering Committee
Approval Date: November 4, 2011

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, network traffic, or any Computing Asset at any time for security, network maintenance and policy compliance purposes (see EXCEPTIONS).

3.2.6. The County provides a best effort, technical solution to block access to known Internet sites that contain adult/sexually explicit, gambling and remote Proxy Sites.

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.

3.3.3.1. When authorized, messages can be restored from a backup copy. These procedures are intended for disaster recovery purposes, and not for customer convenience or use when responding to a public records request.

3.3.3.2. Users are expected to work with their department head to determine retention schedules for E-mail that constitutes a final work product or contains information that may need to be provided in response to a public records request.

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 Computing Assets for personal use

3.5.1. The County provides E-mail, Internet services, access to commercial Instant Messaging, telephone services, and other Computing Assets to enable Users to conduct the County's business in an efficient manner. These services and hardware systems are provided for the use 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 Computing Assets for personal use.

3.5.2.1. Users must limit their personal use so that Computing Assets are available for County use at all times.

3.5.2.2. Computing Assets shall not be used for purposes that are in conflict with the County Organizational Values, or in any way contrary to the interests of the County.

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: Personally Identifiable Information, 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 established policies and individual application requirements.

3.6.3. Data Protection

3.6.3.1. Password-protected screensavers, with automatic activation set at 10 minutes or less (of inactivity), are required on all non-public use Computing Assets and Mobile Computing Assets.

3.6.3.2. Mobile Computing Assets 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 Mobile Computing Assets 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. (see ISP Virus Protection Policy)

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 on County Computing Assets. The activities listed below are not exhaustive but attempt to provide a framework for activities that fall into the category of unacceptable use. Prohibited uses include:

3.7.1.1. System Activities

3.7.1.1.1. Any use which violates federal, 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;

http://www.leginfo.ca.gov/calaw.html

3.7.1.1.1.1.2. Any Matter in a manner that violates the San Luis Obispo County Policy Against Discriminatory Harassment or the San Luis Obispo County Workplace Violence Awareness Policy;

3.7.1.1.1.1.3. Any illegal Matter (including child pornography) or sexually explicit images deemed by community standards to be obscene;

3.7.1.1.1.1.4. Materials that are sexually explicit, obscene, vulgar, profane, hateful, harmful, malicious, threatening, hostile, abusive.

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.

3.7.1.1.9. Engaging in activity that is contrary to the interests of the County.

3.7.1.1.10. Engaging in activity for personal profit including commercial activities and solicitation, conducting personal business interests, or pursuing business interests for other individuals or organizations.

3.7.1.1.11. Engaging in gambling or on-line gaming.

3.7.1.1.12. Using a County Computing Asset to knowingly engage in viewing, reading, creating, conveying, downloading, transferring, transmitting, scanning, or printing materials that are inconsistent with the Organizational Values of the County of San Luis Obispo which include; Integrity, Collaboration, Professionalism, Accountability, and Responsiveness.

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 unauthorized 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
1.9	Nov. 4, 2011	All	Changes to include Mobile Computing Assets and, Page 8 – E-mail public records request; Page 9 Clean-up of personal use language and add Organizational values; Page 12 -–Engaging in activity that is contrary to the interests of the County.
1.8	Apr, 8, 2011	3.7 Unacceptable Use	Several minor edits; reference to the Workplace Violence Awareness Policy (3.7.1.1.1.1.2); Added 3.7.1.1.1.1.4, 3.7.1.1.9 (for profit), 3.7.1.1.10 (gambling), 3.7.1.1.11 (Org Values)
1.7	Sep. 23, 2010	3.2.6	Added the County's blocking of sites
1.6	Apr. 2, 2010	3.6.1, 3.6.3.2,3.6.4	Added PII, Added Portable Computing Devices
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 *ISP Acceptable Use Policy*

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

Receiver: You are the sole recipient of this electronic notification. It is recommended that you save the notification electronically or print and file it in the employee's local personnel file.