6.105 - Internet Usage Policy

Effective Date: 07/13/04

PURPOSE

To establish a County information technology (IT) security policy for acceptable use of the Internet utilizing County IT resources.

REFERENCE

July 13, 2004, Board Order No. 10 — Board of Supervisors — Information Technology and Security Policies

Board of Supervisors Policy No. 3.040 — General Records Retention and Protection of Records Containing Personal and Confidential Information

Board of Supervisors Policy No. 6.100 — Information Technology and Security Policy

Board of Supervisors Policy No. 6.101 — Use of County Information Technology Resources, including Agreement for Acceptable Use and Confidentiality of County Information Technology Resources (Acceptable Use Agreement) , attached thereto

Board of Supervisors Policy No. 6.104 — Electronic Communications

Board of Supervisors Policy No. 6.109 — Security Incident Reporting

Board of Supervisors Policy No. 9.015 — County Policy of Equity

Health Insurance Portability and Accountability Act (HIPAA) of 1996

Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009

California Civil Code Section 1798.29

POLICY

This policy is applicable to all County IT users.

County Internet services are provided as a County IT resource for conducting County business purposes. Any other use must be minimal or incidental and may not be a use which is substantial enough to result in a gain or advantage to the user or a loss to the County for which a monetary value may be estimated.

County IT resources, including without limitation County Internet services, may not be used:

- For any unlawful purpose;
- For any purpose detrimental to the County or its interests;
- For personal financial gain;
- In any way that undermines or interferes with access to or use of County IT resources for official County purposes;
- In any way that hinders productivity, efficiency, customer service, or interferes with a County IT user's performance of his/her official job duties;
- To express or imply sponsorship or endorsement by the County, except as approved in accordance with Department's policies and procedures; or

- For personal purpose where activities are for private benefit or advantage, or an outside endeavor not related to County business purpose. Personal purpose does not include the incidental and minimal use of County IT resources, such as occasional internet usage for personal purposes.

Unless specifically authorized by County management, sending, disseminating, or otherwise exposing and/or disclosing any non-public County information (e.g., software program code; business data, documentation or other information; personal data, documentation or related information; any confidential, legislative, or sensitive data, documentation, and other information) is prohibited in accordance with Board of Supervisors Policy No. 3.040 (see Reference section). This includes, without limitation, information protected from disclosure under HIPAA, the HITECH Act, or any applicable information confidentiality or privacy policy or legislation.

Except as expressly authorized below in this Board of Supervisors Policy No. 6.105, no County IT user shall access or use County IT resources to create, exchange, publish, or distribute in public forums (e.g., blog postings, bulletin boards, chat rooms, Twitter, Facebook, MySpace, and other social networking services) any information (e.g., personal information, confidential information, political lobbying, religious promotion, and opinions) not specifically approved by designated County Department management.

County Departments may adopt and implement departmental policies and procedures for authorizing one or more specified individuals, as a part of each such individual's assigned job function, to use County IT resources to create, exchange, publish, or distribute in public forums (e.g., blog postings, bulletin boards, chat rooms, Twitter, Facebook, and other social networking services) information on behalf of the County Department that is not specifically approved by designated County Department management. Such departmental policies and procedures shall, at a minimum:

a) Require all information created, exchanged, published, or distributed otherwise to be in compliance with all applicable aspects of countywide County IT resources policies, standards, and procedures and countywide County IT security policies, standards, and procedures, as well as any additional policies, standards, and procedures established by the County Department;

b) Require the County Department to designate management to regularly monitor the information created, exchanged, published, or distributed in public forums by the specified individual(s); and

c) Require the County Department as quickly as practicable to address instances in which the specified individual(s) do not comply with the departmental policies and procedures.

No County IT user shall store County information (i.e., personal, confidential (e.g., social security number, medical record), or otherwise sensitive (e.g., legislative data) on any Internet storage site without prior written approval by designated County Department management.

No County IT user of County Internet services shall intentionally or through negligence damage, interfere with the operation of, or prevent authorized access to County IT resources.

County IT users must obtain designated County Department management approval to use County Internet services. Authorized users must not share their credentials, usernames, passwords, or allow another person to access County Internet services using their account.

Access to County Internet services is provided, as needed, at the discretion of each County Department. Access to County Internet services is a privilege, which access may be modified or revoked at any time, without notice or consent by designated County Department management.

County IT users cannot expect any right to privacy when using County Internet services. Having no expectation to any right to privacy includes, for example, that County IT users' access to, and use of, County Internet services may be monitored or investigated by authorized persons at any time, without notice or consent.

The County has the right to administer any and all aspects of access to, and use of, County Internet services, including, without limitation, monitoring sites visited by County IT users on the Internet,

monitoring email sites, chat groups and newsgroups, reviewing data downloaded from or uploaded to the Internet by County IT users, and limiting access only to those sites required to conduct County business.

Monitoring the access to, and use of County IT resources by County IT users must be approved in accordance with applicable policies and laws on investigations. If any evidence of violation of this policy is identified, the Auditor-Controller's Office of County Investigations must be notified immediately.

The following are examples of inappropriate access or use of County IT resources, including without limitation County Internet services. This is not a comprehensive list of all possible violations:

- Downloading, accessing, storing, displaying or distributing software, unless approved by designated County Department management
- Downloading, accessing, storing, displaying, viewing or distributing material (e.g., movies, music, software, and books) in violation of copyright laws
- Downloading, accessing, storing, displaying, viewing or distributing pornography or other sexually explicit material
- Soliciting participation in, or advertising scams (e.g., spamming, pyramid schemes, and "make-money-fast" schemes) to others
- Posting or transmitting libelous, defamatory, fraudulent, or confidential information
- Operating a private business or a non-County business related web site
- Posting or transmitting to unauthorized persons any material deemed to be confidential, personal, or otherwise protected from disclosure
- Participating in partisan political activities
- Attempting unauthorized access to the account of another person or group on the Internet, or attempting to circumvent County security measures, or security measures taken by others connected to the Internet, regardless of whether or not such attempts are successful or result in corruption or loss of data or other information (e.g., password stealing, phishing, or whaling).
- Knowingly or carelessly distributing malicious code to or from County IT resources
- Accessing, creating, or distributing (e.g., via email) any offensive materials (e.g., text or images which are sexually explicit, racial, harmful, or insensitive) on County IT resources (e.g., over County-owned, leased, managed, operated, or maintained local or wide area networks; over the Internet; and over private networks), unless authorized to do so as a part of such County IT user's assigned job function (e.g., law enforcement).

Definition Reference

As used in this policy, the term "County IT resources" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 — Information Technology and Security Policy.

As used in this policy, the term "County IT user" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 — Information Technology and Security Policy.

As used in this policy, the term "County IT security" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 — Information Technology and Security Policy.

As used in this policy, the term "County Department" shall have the same meaning as set forth in Board of Supervisors Policy No. 6.100 — Information Technology and Security Policy.

As used in this policy, the terms "personal information" and "confidential information" shall have the same meanings as set forth in Board of Supervisors Policy No. 3.040 — General Records Retention and Protection of Records Containing Personal and Confidential Information.

~~Compliance~~

~~County employees who violate this policy may be subject to appropriate disciplinary action, up to and including discharge, as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.~~

~~Policy Exceptions~~

~~Requests for exceptions to this Board of Supervisors (Board) policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO), and shall require approval by the Board. County Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests, confer with the requesting County Department, and place the matter on the Board's agenda along with a recommendation for Board action.~~

~~RESPONSIBLE DEPARTMENT~~

~~Chief Executive Office~~

~~DATE ISSUED/SUNSET DATE~~

~~Issue Date: July 13, 2004~~	~~Sunset Date: July 13, 2008~~
~~Review Date: August 25, 2008~~	~~Sunset Date: July 13, 2012~~
~~Review Date: July 19, 2012~~	~~Sunset Date: January 13, 2013~~
~~Review Date: June 27, 2013~~	~~Sunset Date: September 30, 2013~~
~~Review Date: September 18, 2013~~	~~Sunset Date: January 30, 2014~~
~~Review Date: January 15, 2014~~	~~Sunset Date: February 28, 2014~~
~~Review Date: February 19, 2014~~	~~Sunset Date: March 19, 2014~~
~~Review Date: March 19, 2014~~	~~Sunset Date: December 31, 2014~~
~~Review Date: January 6, 2015~~	~~Sunset Date: December 31, 2018~~