Monterey County

Subject: Appropriate Use Policy
Date Issued: May 13, 2014
Issued by: Information Technology Governance Committee
Approved by: The County of Monterey Board of Supervisors
Applies to: All County Officials, Employees and Affiliates

2. INFORMATION TECHNOLOGY APPROPRIATE USE POLICY

2.1.1. POLICY PURPOSE

2.1.1.1. This policy outlines permissible use of information technology equipment and information resources in the County. It governs the conduct of persons granted the privilege of access to County information technology resources, whether at a County facility or elsewhere, and refers to all information resources whether individually controlled or shared, standalone or networked.

2.1.1.2. This policy is intended to facilitate access for County officials, employees, affiliates, and constituents to both internal and external information and to promote accomplishment of the objectives of the project or task(s) for which access was granted. It is intended, also, to avoid inappropriate, illegal or unauthorized use of information technology equipment or resources. Uses inconsistent with this policy may subject violators to sanctions, as specified below.

2.1.2. DEFINITIONS

2.1.2.1. Affiliates – Includes, but is not limited to, third party contractors, volunteers, advisory and other committee and commission members, vendors, or others associated with the County in order to accomplish County business.

2.1.2.2. Broadcast – the initiation and/or distribution of a message, unrelated to the accomplishment of County business, over an information technology Resource to all devices and users attached to the resource, which has not been directed to a specific subset of devices or users when the technology resource allows the sender of the message to select narrower distribution.

2.1.2.3. Chain E-Mail – Any message, unrelated to the accomplishment of County business, sent to one or more people that asks the recipient to forward it to multiple others.

2.1.2.4. Information Technology Resources – Any information in electronic or audiovisual format or any hardware or software that make possible the storage and use of such information, including electronic mail, local

databases, externally accessed databases, CD-ROM, motion picture film, recorded magnetic media, photographs, and any other digitized information.

2.1.2.5. Network – Workstations and connections of computer workstations to servers or any other computer system through a local or wide area network, Internet, Intranet, or modem connection.

2.1.3. **GENERAL POLICY REQUIREMENTS**

2.1.3.1. All computer information created utilizing County computing resources is the property of the County.

2.1.3.2. All computer use, including Internet use, on County networks shall be monitored.

2.1.3.3. Persons granted access to County computing resources shall not:

2.1.3.3.1. Make copies of any software, information, communication, data, digital media, or other information technology Resource without specific authorization.

2.1.3.3.2. Utilize, allow or request others to utilize County information technology equipment or resources, or confidential information acquired through the use of those resources or equipment, for personal benefit or any other purpose unrelated to the accomplishment of County business.

2.1.3.3.3. Except in the authorized conduct of their work assignment, divulge the contents of any record or report to any person, or provide information about, or lists of, County employees to parties outside the County.

2.1.3.3.4. Knowingly include, or cause to be included, in any record or report a false, intentionally inaccurate, or misleading entry or knowingly alter an existing database, document, or digitized data with false and/or unauthorized information.

2.1.3.3.5. Divulge authentication information or passwords to anyone.

2.1.3.3.6. Provide access to information technology equipment and resources to any individual that is not properly authorized to access them.

2.1.3.3.7. Destroy, alter, dismantle, or disfigure the County's information equipment, technologies, properties, or facilities, including those owned by third parties.

2.1.3.3.8. Modify County information technology equipment, systems files, or software, install software on any County equipment without specific authorization, or change computer information without being the data owner or having authority to change that information.

2.1.3.3.9. Send electronic communications which hide the identity of the sender or misrepresent the sender as someone else.

2.1.3.3.10. Use County information technology equipment or resources in violation of any County policy or local, state, or federal law including but not limited to policies and laws governing privacy, public record, copyright or patent.

2.1.4. **System and Network Activities**

Persons granted access to County computing resources shall not:

2.1.4.1.1. Copy or use software without an appropriate license or right to use.

2.1.4.1.2. Use products on County equipment that are not licensed for use by the County or which 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.

2.1.4.1.3. Reproduce copyrighted material including, but not limited to, digitization, copying or distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, copyrighted digital media files, or install copyrighted software for which the County or the user does not have an active license.

2.1.4.1.4. Remove information technology equipment, system files, or software programs from County premises, unless specifically authorized by department management.

2.1.4.1.5. Play computer games in the County workplace, with the exception of computer games for the purpose of training first-time users on mouse, pointer, or stylus control while the user is in a formal training mode.

2.1.4.1.6. Export software, technical information, encryption software, or technology in violation of international or regional export control laws. Users shall consult with appropriate management prior to exporting any material that is in question.

2.1.4.1.7. Introduce malicious programs into the County network or any County computing device (e.g., viruses, worms, Trojan horses, root kits, e-mail bombs, etc.).

2.1.4.2. **Offensive behavior**

Persons granted access to County computing resources shall not:

2.1.4.2.1. Use County information technology equipment or resources to engage in procuring or transmitting material in violation of sexual harassment or hostile workplace law.

2.1.4.2.2. Send messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, ethnicity, political affiliation, physical attributes, or sexual orientation.

2.1.4.2.3. Transmit, retrieve, or store any communications of a discriminatory or harassing nature or materials that may be perceived as obscene, unless directly related to the conduct of law enforcement activities or investigations.

2.1.4.2.4. Transmit, retrieve, or store abusive, profane, or offensive language or pictures (including all pornography) on the County's network unless required by business necessity (e.g. investigative case evidence) and authorized in writing by department directive.

2.1.4.2.5. Make fraudulent offers of products, items, or services.

2.1.4.2.6. Transmit, retrieve, or store illegal material, such as child pornography, from any source, with the singular exception of job requirements related to the fulfillment of law enforcement responsibilities.

2.1.4.3. **Testing and circumvention of security controls**

2.1.4.3.1. For purposes of this section, "testing and circumvention" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

2.1.4.3.2. Unless approved in advance in writing by the Chief Security and Privacy Officer and performed in coordination with Information Security, persons granted access to County computing resources shall not :

2.1.4.3.2.1. Access data of which the user is not an intended recipient.

2.1.4.3.2.2. Log in to a system or account that the user is not expressly authorized to access.

2.1.4.3.2.3. Test, circumvent, or attempt to compromise computer or communication system security measures.

2.1.4.3.2.4. Use network security scanning or vulnerability assessment tools. This includes the use of such tools for network testing and/or troubleshooting.

2.1.4.3.2.5. Engage in system cracking (hacking), password cracking (guessing), port scanning, security scanning, or similar attempts to compromise security measures.

2.1.4.3.2.6. Use short-cuts bypassing systems security measures, or engage in pranks and practical jokes involving the compromise of systems security measures.

2.1.4.3.2.7. Execute any form of network monitoring that will intercept data not intended for the user.

2.1.4.3.2.8. Test or circumvent, or attempt to compromise user authentication or security of any host, network, or account.

2.1.4.3.2.9. Interfere with or deny service to any user other than the user's host (e.g., denial of service attack).

2.1.4.3.2.10. Use any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable a user's session, via any means.

2.1.4.3.2.11. Utilize any form of network sniffer device or software or configuring sniffing ports on the County's network.

2.1.5. **Electronic Mail (e-mail) and Internet Use**

2.1.5.1. E-mail and Internet access are tools provided to accomplish County business. With the exception described below, private or personal use of e-mail and Internet access unrelated to County business is prohibited.

2.1.5.1.1. Infrequent, brief personal use of e-mail and Internet access is permissible only where it is of such a limited nature that it does not interfere with performance of duties, does not detract from responsiveness to the public, does not result in cost to the County, and does not compromise the security or integrity of County information technology equipment or resources. Ordinarily, such use should occur, if at all, before or after work hours and during employee breaks. Examples of permitted personal use include transmitting e-mail to a family member to assure safe arrival home, confirming health care appointments, or checking traffic conditions for a commute. Examples of prohibited personal use

include online shopping, making personal vacation plans, private postings on blogs, chat rooms and social media sites, and instant messaging.

2.1.5.1.2. Departments may adopt more stringent policy regarding personal use of email and Internet access in order to serve their specific business needs and County functions. Individual Department policy, if any, should be consulted for specific guidance.

2.1.5.2. All e-mail and Internet records transmitted over the County network are County records and shall be transmitted only to individuals who have a business need to receive them. Users shall have no expectation of privacy in personal or business communications over County computers or networks, including fax machines and networked copiers.

2.1.5.3. All messages communicated on the County's e-mail system shall contain the name of the actual sender.

2.1.5.4. Any messages or information sent to another individual or entity outside of the County shall not disclose any confidential or proprietary information to parties with no County business reason to know.

2.1.5.5. County officers, employees and affiliates shall not broadcast e-mail messages to all users without specific authorization by the Department Head or Division Chief. Authorized messages with broad distribution shall minimize the size of the message, limit the size and number of attachments, and restrict the use of embedded images. Any announcement which any user wishes to make utilizing County email that is not strictly related to County business shall be approved in advance by his or her department manager and must be of general interest to County employees as determined by the Department Head or Division Chief.

2.1.5.6. The County's e-mail system may be made available for use by County employees for official union or Association related business, subject to applicable law and regulations, the conditions set forth in this policy, and any agreed upon limitations regarding use. Use is subject to prior written agreement between the Union or Association and the County. Employees using the County's e-mail network for such purposes shall be required to familiarize themselves with and abide by these requirements. Use of the system for union business is restricted in that there shall be:

2.1.5.6.1. No union or Association related messages may be broadcast.

2.1.5.6.2. No confidential or individual-specific information may be communicated, such as information regarding a disciplinary action.

2.1.5.6.3. No messages that might malign the County, its employees, or officials.

2.1.5.6.4. No messages may be used to coordinate any job actions.

2.1.5.7. Sending unsolicited e-mail messages shall be prohibited, including but not limited to the following examples:

2.1.5.7.1. The sending of "junk mail" or other advertising material to individuals who did not specifically request such material (i.e. e-mail spam).

2.1.5.7.2. Any form of illegal harassment.

2.1.5.7.3. Forging of e-mail header information.

2.1.5.7.4. The sending or forwarding of chain e-mail. County officers, employees and affiliates are directed to break the chain, deleting any chain email messages received and requesting the sender to discontinue forwarding mail of this type.

2.1.6. **Telecommunications Equipment Use**

2.1.6.1. Electronic voice communications via telephones, radios, pagers, cell phones, images transmitted via facsimile machines, computers or tablets transmitting audio files as a means of voice communication, and any other related technologies shall be subject to County policy and regulation. It is the responsibility of the person initiating any telecommunication transmission utilizing County information technology resources to ensure that the communication complies with County policy and regulation.

2.1.7. Individual County Departments may define "conditions of use" for more restrictive access to County information technology resources when additional detail, guidelines, and/or restrictions are consistent with this policy and necessary for achievement of the department's mission, goals, objectives, or functions.

2.2. EXCEPTIONS

Under rare circumstances, the County may need to vary from these policies. All such instances shall be approved in writing and in advance by the Director of Information Technology and/or the Chief Security and Privacy Officer. Disputed issues may be escalated to the Information Technology Governance Committee for final decision as necessary.

2.3. ENFORCEMENT

Violators of this policy may be subject to disciplinary action up to and including employment termination, termination of agreements, denial of service, loss of access privileges, and/or additional legal penalties, both criminal and civil. Allegations of violations of Equal Employment Opportunity protections will be referred to the Office of Equal Employment Opportunity for investigation. Reports or complaints of possible illegal material will be investigated by the Department having ownership of the information resources used with consultation from the Information Technology Department, County Counsel, and/or other agencies as appropriate.