SACRAMENTO COUNTY

Adopted Standards and Policies
Information Technology Acceptable Use Policy

To:
Chief Deputy County Executives, Department Directors

From:
Rami Zakaria
Chief Information Officer

Date:
December 2, 2016

Subject:
County of Sacramento Information Technology Acceptable Use Policy

---

It is my pleasure to introduce the new revised Countywide Information Technology Acceptable Use Policy. The Department of Technology developed this policy with input from Department Directors and vetted it through the Department of Personnel Services, County Counsel and recognized employee organizations through the meet and confer process. This policy is designed to be general in nature and departments are encouraged to create a companion policy to meet unique departmental situations.

This policy clarifies appropriate use and ownership of the County's IT resources, data and equipment and includes the following sections:

1. **Software** addresses appropriate licensing and prohibits unauthorized duplication of software and introduction of malicious programs to County IT resources.
2. **County Data** addresses County employees' responsibility to protect sensitive and confidential data and outlines policy for the use of cloud storage.
3. **Offensive Behavior** prohibits access to and transmittal of inappropriate or offensive behavior and content on County IT resources.
4. **Circumvention of Security Controls** prohibits security breaches or disruptions of network communications and outlines prohibited activities.
5. **Electronic Mail (e-mail) and Internet Use** defines appropriate use of County e-mail and messaging and limits expectation of privacy on County IT resources.
6. **Telephone and Mobile Equipment Use** addresses the use of electronic voice communications and sets the policy for mobile device management and security.

Please note this policy requires user Acknowledgement of Receipt and Understanding. The Department of Personnel Services will ensure this is incorporated into the new employee onboarding process and retained in personnel files.

If you have any questions, contact me at 874-7825.

Concurrence: 
Navdeep S. Gill, County Executive

SACRAMENTO COUNTY

Department of Technology

Policy Title: **Information Technology Acceptable Use Policy**

Authority: **Chief Information Officer**

Effective Date: **January 1, 2017**

Purpose:
This policy outlines the acceptable use of Sacramento County's information technology (IT) resources. The County provides IT resources to facilitate our mission, goals and objectives, and must manage them responsibly. These rules protect users and the County and do not intend to inhibit the ability to perform the job. Inappropriate use exposes the County to significant risks including cyber-attacks, data loss, compromise of computer networks, systems and services, and human resource and legal issues.

Scope:
Information technology resources include 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.

This policy applies to any County user. In this document, the term user refers to any employee (permanent or temporary), contractor, consultant, vendor, volunteer, student intern, or other person, who uses, maintains, manages, or is otherwise granted access to County IT resources. This includes access at a County facility or elsewhere, and refers to all IT resources whether individually controlled or shared, standalone or networked.

Information technology resources shall not be used for purposes other than those that support official County business. However, incidental use of the County electronic mail and internet may be permissible, as outlined in this document. Access to and use of the County's IT resources is a privilege, shall be treated as such, and shall be used in a manner that respects the public trust and abides by established policy and regulations. Further, access to the IT resource infrastructure both within the County and beyond requires that each and every user accepts responsibility to protect the rights of other County users and the public they serve.

Policy:
Sacramento County aspires to maintain secure access for its officials, constituents and users to both internal and external information with regard to County government processes, including relevant information garnered from local, state, national, and international sources. In addition,

the County seeks to provide an atmosphere that encourages access to knowledge and information sharing that is consistent with the mission and objectives of County government.

Sacramento County recognizes the importance of reliable information to ensure legal compliance, accountability, and promote open and transparent government. It is essential that users take necessary care when creating or entering data into government systems.

Use of IT resources should be consistent with the job function and specific objectives of the project or task(s) for which access to the resources was granted. All uses inconsistent with the objectives outlined below are considered to be inappropriate and unauthorized use and may jeopardize further access to services and result in disciplinary or legal action.

a. All computer information designs, programs, and data created utilizing County computing resources are the sole property of the County.
b. All computer use, including Internet use, on Sacramento County networks shall be monitored.
c. Each person granted access to County network resources shall be responsible for the content, syntax, and format of all text, audio, or images that he/she may place upon or send over the network. All users shall conduct themselves with the same integrity in electronic interactions as they would in face-to-face dealings with one another and shall not:
    i. Make unauthorized use of any IT resource;
    ii. Make unauthorized copies of any software, license codes, information, communication, data, or digital media;
    iii. Seek personal benefit or permit others to benefit personally from the use of County IT resources or confidential information acquired through the use of those resources. Operate or request others to operate any County IT resource for personal business;
    iv. Exhibit or divulge the contents of any record or report to any person except in the conduct of their work assignment and County policies and regulations;
    v. Provide information about, or lists of, County employees or users to parties outside the County, except as required under the California Public Records Act or as approved by the Department Director or their designee;
    vi. Include knowingly, or cause to be included, in any record or report a false, intentionally inaccurate, or misleading entry, or enter information in a computer file or database that is known to be false and/or unauthorized;
    vii. Divulge personal resource access information or passwords to anyone;
    viii. Provide any non-authorized person access to information or permit such persons the use of County IT resources;
    ix. Use irresponsibly, destroy, alter, dismantle, or disfigure the County's information technologies, properties, or facilities, including those owned by third parties;

x. Make any modification to County computer equipment, systems files, or software, including the installation of any non-standard software on any County workstation, without approval from the Department Director or their designee;
xi. Connect any personal computer, laptop, or tablet to the County network unless using an approved VPN account; exceptions to this may be requested through your Department Director or their designee;
xii. Change computer information without being the data owner or having proper authority to change that information;
xiii. Make copies of County electronic data files without a valid business reason or expressed written approval from the Department Director or their designee;
xiv. Transmit personally identifiable information without encrypting the information when required;
xv. Send electronic communications which hide the identity of the sender or misrepresents the sender as someone else; or
xvi. Jeopardize security, confidentiality, or potentially subject the County to litigation as a result of violating any County policy or local, state, or federal law relative to privacy, public record, copyright, or patent.

System and Network Activities:

1. Software

a. No County owned or licensed software shall be copied or used without an appropriate license or right to use.
b. 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”, personally owned, or other software shall not be used on County equipment.
c. Unauthorized copying of copyrighted material including, but not limited to, digitization, copying or distribution of photographs from magazines, books, Internet web pages or other copyrighted sources, copyrighted music, copyrighted digital media files, and the installation of any copyrighted software for which the County or the end user does not have an active license is prohibited.
d. Use of software shall be in a manner which is prescribed and permitted by the accompanying documentation and licensing agreement(s).
e. Computer equipment, system files, or software programs shall not be removed from County property, reproduced, or used in any way to duplicate software, unless specifically authorized by department management.
f. Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws is illegal, and all users shall consult the appropriate management prior to exporting any material that is in question.

g. Intentional introduction of malicious programs into the network or any computing device (e.g., viruses, worms, Trojan horses, root kits, e-mail bombs, etc.) is prohibited.

2. County Data

It is the duty of each user to protect County data that is designated as sensitive or confidential by the Department Director of the department that owns the data (see the Electronic Data Access Policy). As such, County users will abide by the following policy:

a. County users must use the County's secure, private cloud storage service to store and transfer County data. No public cloud storage services, like Drop Box, Google Drive, or Microsoft OneDrive, may be used for this purpose unless approved by the Department Director or their designee.
b. Use of all private cloud storage services must be formally authorized by the user's supervisor. The supervisor will certify that the user has been properly briefed on County security and privacy policies concerning electronic data.
c. The use of all cloud storage services must comply with all laws and regulations governing the handling of personally identifiable information, Health Insurance Portability and Accountability Act (HIPAA) data or any other data owned or collected by Sacramento County.

3. Offensive Behavior

a. County IT resources shall not be used for procuring, transmitting, retrieving or storing any material or communications that violate County discrimination, sexual harassment, or workplace violence policy.
b. County IT resources shall not be used to access, transmit or retrieve offensive material, or otherwise send or receive offensive material. Offensive material includes, but is not limited to, sexual comments or images, or any comments, pictures, or video that would be offensive on the basis of age, sexual orientation, gender, race, religious beliefs, national origin, or disability.
c. No abusive, threatening, profane, or offensive language or pictures (including all pornography) shall be transmitted through or stored on the County's network unless required by business necessity (e.g., investigative case evidence) and authorized in writing by the Department Director or their designee.
d. Illegal material, such as child pornography, from any source, with the singular exception of job requirements related to the fulfillment of law enforcement or legal responsibilities, is prohibited.

4. Circumvention of Security Controls

a. Unless approved in advance and in writing by the Chief Information Officer and performed in coordination with Information Security, all forms of security breaches or disruptions of network communication are prohibited. Disruption includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes. Prohibited activities include, but are not limited to:

i. Accessing data of which the user is not an intended recipient;
ii. Logging in to a system or account that the user is not expressly authorized to access;
iii. Testing, or attempting to compromise computer or communication system security measures;
iv. Using of network security scanning or vulnerability assessment tools, this includes the use of such tools for network testing and/or troubleshooting;
v. System cracking (hacking), password cracking (guessing), port scanning, security scanning, or similar unauthorized attempts to compromise security measures;
vi. Bypassing systems security measures with short-cuts, as well as pranks and practical jokes involving the compromise of systems security measures;
vii. Executing any form of network monitoring that will intercept data not intended for the user;
viii. Circumventing user authentication or security of any host, network, or account;
ix. Interfering with or denying service to any user other than the user's host (e.g., denial of service attack);
x. Using 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; or
xi. Utilizing any form of network sniffer device or software or configuring sniffing ports on the County's network.

5. Electronic Mail (e-mail) and Internet Use

a. Users' communications on County electronic systems shall be professional, and inoffensive to reasonable individuals or groups.
b. E-mail and Internet access is provided for County business use; incidental use for informal and/or personal purposes maybe permissible only within reasonable limits. Departments may have more stringent policies regarding this use and these policies should also be consulted for specific guidance.
c. Users shall not use County IT resources for commercial financial gain or to conduct and support personal business ventures.
d. All e-mail and Internet data transmitted over the County network is considered County data and shall be transmitted only to individuals who have a business need to receive

them. Users shall have no expectation of privacy in personal communications over County computers or networks, including facsimile machines.

e. All business information contained in County e-mail and Internet shall be accurate, appropriate, and lawful.
f. All messages communicated on the County's e-mail system shall contain the name of the sender.
g. Any messages or information sent to another individual outside of the County shall not disclose any confidential or proprietary information to parties unauthorized to view.
h. Users shall not broadcast e-mail messages to all County users without specific authorization by the County Executive's Office. E-mail messages shall not be sent to large distribution lists, entire Departments, Divisions or Programs without authorization by the Department Director or their designee. 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 e-mail that is not strictly related to County business shall be approved in advance by his or her Department Director or their designee and shall only be of general interest to County users.
i. Access to the County's e-mail system for union or Association business shall be no less than allowed for other non-business communication as spelled out in this policy.
j. The County standard instant messaging tool may be used in lieu of telephone conversation. Instant messaging sessions require the same courtesy and legal consideration as e-mail messages.

6. Telephone and Mobile Equipment Use

a. Electronic voice communications via telephones, radios, pagers, cell phones, images transmitted via facsimile machines, and any other related technologies shall be subject to the County policy and regulation as referenced below in this document and contained in this policy.
b. Mobile phones, smartphones, tablets, Wi-Fi hotspots purchased by the County are to be used to support official County business. Incidental use of these resources for personal purposes is permitted within reasonable limits. If personal use of a County device results in any additional cost to the County, the department may require the user reimburse the County for those costs. County departments may create additional policies to further refine or restrict the use of mobile devices.
c. For County owned smartphones and tablets, the County standard mobile device management software will be installed so that all of its data can be remotely erased when it is lost, stolen, or no longer in use.
d. The County does not require users to use their personal mobile devices to conduct County business. If users choose to use their personal devices to connect to a County network, or access County e-mail they must adhere to the following requirements:

i. Lock the device with a minimum four character password when it is not in use.
ii. Utilize an inactivity timeout of no more than 15 minutes whereby the user must enter their password to unlock the device.
iii. Take reasonable precautions to secure the mobile electronic device from loss or theft.
iv. Allow the mobile phones to be remotely erased of its data when it becomes lost, stolen or is no longer used for County business.

e. When a mobile device that is used for County business is lost, stolen, or no longer used for County business, users must immediately report the loss to the IT Service Desk and their Departmental cell phone coordinator.
f. In certain applications voice transmissions may be recorded and monitored for appropriateness, documentation, and/or training purposes. It is the responsibility of the person initiating any telecommunication transmission utilizing County IT resources to ensure that the content, syntax, and format of the communication comply with County policy and regulation as referenced below in this document and contained in this policy.
g. Individual County departments may define "conditions of use" for more restrictive access to County IT resources when additional detail, guidelines, and/or restrictions are consistent with this policy and necessary for achievement of the department's mission, goals, initiatives, or functions.

Enforcement:
Violators of this policy may be subject to disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil. Reports or complaints of possible violation of this policy will be investigated by the Department of Personnel Services in collaboration with the department having ownership of the IT resources used with consultation from the Department of Technology, and/or other departments as appropriate.

References:

- Sexual Harassment Policy
- Discrimination Policy
- Workplace Violence Policy
- Information Technology Standards
- Electronic Data Access Policy

Definitions:

- Broadcast – the initiation and distribution of a message 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 such a narrower distribution.

- Incidental use –personal use of an information technology resource before work, after work, during breaks and lunch that does not interfere with completing work assignments.
- Information Technology (IT) 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.
- 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.
- User – any employee (permanent or temporary), contractor, consultant, vendor, volunteer, student or other person who uses County-owned or leased information technology resource.

Exceptions:
The Chief Information Officer acknowledges that under rare circumstances, certain users will need to employ systems that are not compliant with these policies. All such instances shall be approved in writing and in advance by the Chief Information Officer. Issues may be escalated to the County Executive for final decision as necessary.

Approved by: **County Executive**

Acknowledgement of Receipt and Understanding
I hereby certify that I have read and fully understand the contents of the IT Acceptable Use Policy. Furthermore, I have been given the opportunity to discuss any information contained therein or any concerns that I may have. My signature below certifies my knowledge, acceptance and adherence to the County of Sacramento IT Acceptable Use Policy.

Signature: _____ Date: _____