Resolution 2016-034

BOARD OF SUPERVISORS
COUNTY OF SIERRA
STATE OF CALIFORNIA

A RESOLUTION UPDATING THE SIERRA COUNTY INFORMATION TECHNOLOGY (IT) POLICY

WHEREAS, the Board of Supervisors previously adopted an Electronic Media and Use Policy pursuant to resolution 2009-067, governing the appropriate uses, processes, and procedures by which county employees shall use the County's electronic media and devices,

WHEREAS, electronic media and devices are a topic of constantly evolving practical, technical, and legal requirements and best practices,

WHEREAS, on March 1, 2016 the Board indicated its intent to adopt an updated policy pertaining to electronic media and other forms of information technology after further drafting and review by staff,

WHEREAS, the attached Information Technology Policy has been reviewed and edited by staff pursuant to the Board's direction,

NOW THEREFORE BE IT RESOLVED

The attached Information Technology (IT) Policy, dated April, 2016, is hereby adopted by the County of Sierra. This policy shall supplant and supersede any prior County policy on the same subject matter.

ADOPTED by the Board of Supervisors of the County of Sierra, State of California on the 5th day of April, 2016 by the following vote:

Ayes: Supervisors Huebner,Roen,Beard,Schlefstein,Adams
Noes: None
Abstain:None
Absent: None

County of Sierra

Lee Adams, Chairperson
Board of Supervisors

Attest:

Heather Foster
Clerk of the Board

Approved as to Form:

James Curtis
County Counsel, by
Christian Curtis,
Deputy County Counsel

Resolution 2016-034

Sierra County

Information Technology Policy

April 2016

Table of Contents

Page No.

Purpose

Information and the systems, networks, and software necessary for processing are essential Sierra County assets that must be appropriately protected against all forms of unauthorized access, use, disclosure or modification. Security and controls for County information and associated assets (County I/T Assets) must be implemented to help ensure privacy, confidentiality, data integrity, availability, accountability, and appropriate use. This policy establishes the minimum standard to which all departments must adhere. Departments may, with the approval of the Information Systems Department (IS Department), enhance the minimum standard based on their unique requirements.

Policy

1. Definitions

"County I/T Assets" include, but are not limited to, the following:

- Computers and any electronic device that stores and/or processes County data (for example: desktops, laptops, midrange, mainframes, PDA's, County wired or wireless networks, digital cameras, copiers, IP phones faxes, pagers, related peripherals, etc.)
- Storage media (diskettes, tapes, CDs, zip disk, DVD, etc.) on or off County premises
- Network connections (wired or wireless) and infrastructure, including jacks wiring, switches, patch panels, hubs, routers, etc.
- Data contained in County systems (databases, emails, document repositories, web pages, etc.)
- County purchased, licensed, or developed software

"Department" means the department in which an employee's job position is assigned. For elected officials, "Department" means the departments for which they are the appointing and/or elected official.

"Electronic devices" include, but are not limited to, the following:

- Any electronic device which communicates, sends, receives stores, reproduces or displays voice and/or text communication or data, such as cellular phones, pagers, smart phones, music and media recorders and players, gaming devices, tablets, laptop computers and personal digital assistants.

"Employees" for the purposes of this policy include only the following:

- County elected officials
- County appointed officials
- County employees

"Network" includes, but is not limited to all electronic systems developed by and used by the County, including the County's website, electronic mail, the internet, telephone communications, radio communications, and facsimile transmissions.

"Personal devices" are any electronic devices not owned by the County.

2. Responsibilities

Departments, Commissions, Board and Offices

Departments are responsible for ensuring appropriate use and security of County I/T Assets within the Department. Departmental management is responsible for organization adherence to this Policy, any other applicable technology and security policies, and any further direction by the IS Department. Departments must ensure that all of their respective employees be made aware of this Policy, any other applicable technology and security policies, and any further direction by the IS Department; and that compliance is mandatory.

Departmental management is responsible for developing organizational procedures in consultation with the IS Department to support policy implementation, including departmental policy regarding the retention and deletion of electronic data.

The Department Head will ensure the designation of an individual to be responsible for coordinating appropriate use and information security within the Department.

Information Systems Department

The IS Department is responsible for ensuring that the County I/T Assets operate at maximum efficiency and are available to all authorized users at all authorized locations at all authorized times. In doing so, the IS Department will do the following:

- Implement this Policy, as well as any other County technology policies unless otherwise directed by the Board of Supervisors;
- As technology and safety requirements change, the IS Department will review and propose revisions of this Policy, and any other County technology policies, to the Board of Supervisors;
- Develop, implement, review, and recommend additional technology policies that the IS Department deems advisable;
- Manage County I/T Assets;

- Develop, review, revise and lead County I/T Assets trainings and education efforts;
- Assist in the development of, and approve, department-specific technology procedures and policies;
- Identify and stay abreast of industry best practices regarding technology, including but not limited to, information security;
- Assist in the development of, and approve, inter-departmental, collaborative use of County I/T Assets;
- Acquire and place into operation the best technology available that is compatible with County resources and needs of County citizens and employees;
- Maintain County I/T Assets to ensure they operate at maximum efficiency, and that all authorized users at all authorized locations are supplied with high quality voice and data processing and internet access at all authorized times;
- Endeavor to ensure standardization of operating systems and applications in an effort to restrain costs, encourage efficiencies, generate synergies, and prevent the development of indispensability in so far as this is possible;
- Protect County I/T Assets from injury, whether such injury originates internally or externally; and
- Set priorities, subject to the approval of the Board of Supervisors, for the use of County I/T Assets for the benefit of the greatest number for the greatest good. Emergency services will always receive the highest priority.

Employees

Employees are responsible for adhering to this Policy, any other applicable technology policies, and any further direction by the IS Department. Employees are responsible for protecting County I/T Assets for which they are entrusted and using them for their intended purposes.

3. Access Control of County I/T Assets

Accessing County I/T Assets is strictly prohibited unless expressly authorized by the Board of Supervisors, IS Department, or departmental management.

Unauthorized access to any County I/T Assets, including but not limited to, the computer system, network, software application programs, data files and restricted work areas and County facilities is prohibited.

The IS Department will develop, review and revise access control mechanisms to protect against unauthorized use, disclosure, modification, or destruction of resources.

Authorized users may not share any login identification information with any other person absent written authorization from the IS Department or departmental management. This prohibition includes, but is not limited to sharing user names, passwords, electronic cards, biometric logons, secure identification cards, and/or other authentication mechanisms.

All workstations are to use the IS Department-established Microsoft Office Suite configuration.

Some workstations may, with prior approval of departmental management and the IS Department, be allowed to have department-specific applications as long as these do not cause conflicts. After consulting with departmental management, the IS Department is authorized to remove any non-approved applications, including screen savers, from any workstation connected to the County network.

Department management will direct to the IS Department which accounts are to be created on which workstations and which files and applications the account will be able to access on identified workstations.

All passwords will be updated by the IS Department no later than January 31st of each year.

Only specific accounts are to be allowed on each department's shared files. Departmental management will inform the IS Department which accounts are permitted to access identified files and/or folders.

The doors to the two computer rooms are to remain locked except when authorized persons are in these rooms.

No person is to approach the phone blocks and junction area in the basement without first checking in with the IS Department.

An updated version of the virus protection selected by the County will be loaded onto each workstation by the IS Department.

All servers will be backed up on a schedule set by the IS Department. Back-up tapes will be distributed and stored in a fire-proof container.

The halFILE System will be backed up with both tapes (whole system) and compact disks (CDs). One copy of each CD will be stored in a fire-proof container.

Users may not use any unauthorized cloud environment for the storage or transmittal of County data. The use of a specific cloud environment must be approved in advance by departmental management after approval by the IS Department. Approved cloud environments will not be used as the sole or primary means of storing County data.

The IS Department will develop, implement, review and revise a software management program. The program will include the documentation of license numbers, serial numbers, dates of purchase, and log warranty expiration dates for all purchased software. The program will also include the tracking of license expiration and ensure timely renewal of all software license agreements.

Virtual Private Network Access

VPN access is permitted to County employees only.

No employee will be provided with VPN access without specific written consent from their Department Head and the IS Department. Departmental management is responsible for contacting the IS Department to receive/complete/file the Virtual Private Network Use Agreement.

Once the required Agreement has been filed with the IS Department, the IS Department will provide the authorized employee virtual access to the network. No employee may access the County network other than through the use of a County-owned and County-monitored computer. If the requesting department does not have a County-owned and county-monitored computer available, the Department will contact the IS Department to determine if one is available elsewhere. Departments that have County-owned and County-monitored computers must ensure those computers are plugged into the County network bi-monthly to receive security and software upgrades.

All VPNs must have their own point of contact security.

All use of VPN access must comply with applicable privacy laws and maintain confidentiality at all times.

Authentication

Access to County I/T Assets is based on an appropriate user authentication mechanism, as determined by the IS Department, according to the sensitivity and level of risk associated with the data.

All County I/T Assets containing restricted-access data must require user authentication before granting access.

Users may not allow others to access County I/T Assets if that asset is assigned to the users, or when that asset is logged into the County network under the users' identity.

Users are prohibited from representing themselves as another person, real or fictional, or anonymously when using County I/T Assets, unless otherwise required by their job duties.

New Employee Network Access

Department management must request new employee access to the County network by submitting an Offer of Employment Form in the ReadyDesk ticketing system no later than seven

(7) days prior to the employees' start date. Upon receipt, the IS Department will provide a copy of the form to the Auditor's Office. It is the responsibility of departmental management to maintain the ReadyDesk ticket for new employee access.

Terminating Employee Network Access

Departmental management must request termination of employee access to the County network by submitting a Termination Request Form to the IS Department.

To the extent possible, departmental management must notify the IS Department of any employee termination prior to giving notice to that employee to ensure protection of County I/T Assets.

4. Official Use of County I/T Assets

County I/T Assets are to be used exclusively for County business purposes, except as stated in Section 5.

Use of County I/T Assets is limited to County employees unless otherwise authorized by the Board of Supervisors.

No user may intentionally, or through negligence, damage, interfere with the operation of, or prevent authorized access to County I/T Assets. It is every user's duty to use County I/T Assets responsibly, professionally, ethically, and lawfully.

No user may remove or alter any signature block, watermark, or other information or data automatically populated into a communication, document, or other data field by the network.

The County has the right to administer any and all aspects of access and use of its I/T Assets, including the right to monitor internet, electronic mail, data and all other forms of access.

Any monitoring or investigation of employee access to, and/or use of, County I/T Assets, including but not limited to internet, electronic mail and data files, must be approved by the Board of Supervisors or departmental management. If evidence of abuse is identified, notice must be provided immediately to the IS Department, and the Risk Management Office.

Users should not expect any privacy in anything they create, store, send, receive, or use in conjunction with using County I/T Assets.

Use of County I/T Assets may be considered a public record subject to discovery under California law.

Data Integrity

Users are responsible for maintaining the integrity of County data. Users may not knowingly or through negligence cause County data to be modified or corrupted in any way that compromises its accuracy or prevents authorized access.

Electronic Mail and Internet Access

Electronic mail and internet access is provided as County I/T Assets for conducting County business. Electronic mail and internet access are to be used for County business purposes only.

Access to County electronic mail and internet access is a privilege that may be wholly or partially restricted without prior notice or without consent to the user.

Access to County electronic mail during non-business hours without specific written approval of departmental management is strictly prohibited.

All electronic mail messages, including any attachments thereto, are the property of the County and subject to review by authorized County personnel.

All data and information downloaded from County internet access is the property of the County and subject to review by authorized County personnel.

The County has the right to administer any and all aspects of access and use of its electronic mail and internet access, including the right to monitor internet, electronic mail and data access, monitoring sites visited by users, monitoring chat groups and newsgroups access by users, and reviewing materials downloaded from or uploaded by users.

Users should not expect any privacy in anything they create, store, send, receive, or use in conjunction with using County electronic mail and/or internet access.

Personal Devices

Only employees selected by their Department Head are authorized to use a personal device to access County I/T Assets.

Unauthorized persons may still use personal devices to connect to Wi-Fi networks designated by the County for public access.

Any personal device to be used to access County I/T Assets must be compatible with County I/T Assets and have the pre-approval of the IS Department.

Authorized personal devices accessing County I/T Assets must use secure authentication and strong encryption methods established, managed and controlled by the IS Department.

Any person who uses a personal device to access County I/T Assets must use such devices appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of the user access to County I/T Assets and immediate removal of all County data from the device.

The IS Department may deny access to County I/T Assets by personal devices for any action deemed by the IS Department to be a risk to the County I/T Assets and users.

The IS Department reserves the right to establish and enforce access methods to County I/T Assets.

The IS Department reserves the right to manage security policies, network application and data access centrally where appropriate and necessary. Any attempt to contravene or bypass County security measures will be deemed an intrusion attempt and the device will be blocked and the user account suspended.

Authorized users will follow all data removal procedures to permanently remove County specific data from personal devices once the person is no longer authorized to access County I/T Assets.

If an authorized personal device is lost or stolen, the user must report the incident to the IS Department immediately. In the event of a lost or stolen personal device, the County will take steps to ensure that access to County data is secured, potentially including but not limited to, password changes and account suspension, along with remote removal of all County access and data from the device.

The IS Department reserves the right to establish audit trails and logs to locate personal devices with access to County I/T Assets, and such information may be used to investigate usage.

Personal devices with access to the County I/T Assets may not be used in any way that is not designed or intended by the device manufacturer, including but not limited to "jailbreaking" and "rooting" devices.

County employees required by their Department Manager and approved by the Board of Supervisors to use a personal device for County related purposes will be provided an allowance for the purpose of offsetting the costs for County use of the device. The employee receiving such an allowance will be solely responsible for the costs of private ownership including but not limited to the purchase, activation, maintenance, support, monthly usage, late fees, interest, term commitments and replacement of such devices and any increase in personal income tax liability. Any employee who receives an allowance may add extra services, equipment or features as desired at his/her own expense.

Any County employee who receives an allowance must maintain active service while receiving the allowance. The personal device must be readily available for two-way communication during normal work hours, approved overtime hours, when responding to an emergency, and/or when placed on standby or call-back pay status.

Portable Devices

All portable devices holding confidential County data, including but not limited to, external hard drives, and flash (thumb) drives, must be encrypted. Departments will be required to log the assignment of all portable devices including:

- Employee name
- Date assigned
- Date returned

External auditors and/or contractors working for the County may be excluded from this requirement.

Social Media

Department use of social media technology must conform to the policies, protocols and procedures contained, or referenced, herein.

Social media applications used by Departments must be approved by the Board of Supervisors prior to use.

Privacy

Information accessed using County I/T Assets must be used for County authorized purposes only, and must not be disclosed to third persons without written authorization from departmental management.

Confidentiality

Unless expressly authorized by departmental management or policy, any sending, disclosing, or other dissemination of confidential or protected information is strictly prohibited.

Viruses

If a user discovers, or fears, that a virus has infected a County I/T Asset, the user may not send any further communications with that asset, or use that asset in any way. The user must contact the IS Department by other means of communication immediately. The IS Department will scan the effected device, and return the device to the user only if any virus or other contagion is effectively removed.

Electronic Disposal

All data, with the exception of native data initially installed by the manufacturer, must be permanently removed from any County I/T Asset before possession and/or ownership of the County I/T Asset may be transferred from the County.

All data from a County I/T Asset may be removed, temporarily or permanently, as directed by the IS Department.

The IS Department is responsible for removing data from County I/T Assets. Employees must surrender all County I/T Assets as directed by the IS Department.

The IS Department is responsible for the disposition of all County I/T Assets subject to the approval of the Board of Supervisors. All County I/T Assets that become the responsibility of the IS Department for the purpose of disposal must be logged onto the Electronic Data Disposal Verification log maintained by the IS Department.

Disposal of County I/T Assets must comply with all federal, state, County, and applicable local laws, including but not limited to environmental regulations.

5. Incidental Personal Use of County I/T Assets

Notwithstanding any other part of this Policy, incidental personal use of County I/T Assets is permitted so long as employee use is made during the time the employee is relieved from duty (i.e. during a break, during the employee's lunch hour, or before or after the employee's work shift), so long as the Department Head determines that the operation of the Department is not being compromised or disrupted, and subject to the additional requirements set forth herein.

Incidental personal use must not:

1. Interfere with the County operations;

2. Interfere with the user's duties to the County; nor

3. Incur any additional costs to the County other than de minimis in nature.

Any incidental use of the County I/T Assets should clearly indicate that the use is personal. While engaging in incidental personal use, users may not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the County. The County is not responsible for any loss or damage incurred by an individual as a result of personal use of County I/T Assets.

Personal use of the County electronic mail network is prohibited at all times, including any incidental use. However, employees may use the County internet access to check personal, web-based email accounts such as gmail.com and hotmail.com.

Prohibited Activities

Prohibited personal incidental use of County I/T Assets include, but are not limited to, the following:

1. Any use that violates federal, state, County, or applicable local laws, regulations rules, policies or procedures.

2. Any use for an offensive or harassing purpose.

3. Any unauthorized access of County I/T Assets or other County property.

4. Any unauthorized access, use, alteration, and/or removal of any material or communication.

5. Any use intended to accomplish or assist in unauthorized access of County I/T Assets or other County property.

6. Any use intended to accomplish or assist in unauthorized access, use, alteration, and/or removal of any material, or communication.

7. Any transmittal or downloading of any material or communication which includes potentially offensive material (such as sexually explicit, racial, defamatory, profane, threatening, ethnic comments, jokes or slurs).

8. Any misrepresentation of an employee's true identity.

9. Any unauthorized downloading, accessing or transmittal of information, documents or software, including any acts that infringe copyright.

10. Any use of software not in compliance with license agreements and as authorized by the IS Department.

11. Any use which causes the County to incur a fee for which there has not been prior approval.

12. Any use of a security code or password other than as authorized.

13. Any disclosure of login identification information to anyone other than the IS Department.

14. Any use for the purpose of private remuneration.

15. Any use that suggests County endorsement of personal communications.

16. Any transmittal of unauthorized broadcast communications or solicitations, such as mass email transmittals. All broadcast or solicitation messages must be approved in advance by departmental management and/or the IS Department.

17. Any use of the County's data processing network that interferes with the ability of the employee or other users to conduct County work. This includes, but is not limited to, downloading or uploading software, games, or shareware.

Compliance

Unauthorized use of County I/T Assets will have the same consequences as the misuse of any County property.

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge, denial of access, and/or civil and criminal penalties. Contractors and other non-employees may be subject to termination of any contractual agreements, denial of access, and/or civil and criminal penalties.

6. Electronic Data Retention

Electronic messages stored on the County exchange server will automatically be deleted after six (6) months on the active electronic mail server.

The IS Department will develop, implement, review and recommend any additional electronic data standards it deems necessary subject to the approval of the Board of Supervisors.

7. Requesting Assistance from IS Department

Persons requesting assistance from the IS Department must submit a ReadyDesk Ticket. However, if the assistance is for an employee termination the respective department manager must submit a *Termination Request Form* directly to the IS Department.

Policy Exceptions

Requests for exceptions to this Policy must be reviewed by the IS Department and approved by the Board of Supervisors. Departments requesting exceptions should provide such requests to the IS Department. 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 department, initiatives, actions and a time frame for achieving the minimum compliance level with the policies set forth herein. The IS Department will review such requests, confer with the requesting department and place the matter on the Board of Supervisor's agenda along with a recommendation on the request.

00444931.DOC