# Sierra County
## Board of Supervisors’
### Agenda Transmittal & Record of Proceedings

**MEETING DATE:**
March 1, 2016

**TYPE OF AGENDA ITEM:**
☒ Regular  ☐ Timed  ☐ Consent

**DEPARTMENT:** Information Systems

**APPROVING PARTY:** Laura A. Marshall

**PHONE NUMBER:** 530-289-3283

### AGENDA ITEM:
Resolution adopting Sierra County Information Technology Policy

### SUPPORTIVE DOCUMENTS ATTACHED:
- ☒ Memo
- ☒ Resolution
- ☐ Agreement
- ☒ Other

Resolution, Sierra County Information Technology Policy

### BACKGROUND INFORMATION:
This policy will replace the Electronic Media and Use Policy adopted by the Sierra County Board of Supervisors on May 19, 2009, at Resolution 2009-067.

### FUNDING SOURCE:
N/A

### GENERAL FUND IMPACT:
No Additional General Fund Impact

### OTHER FUND:
- AMOUNT: $ N/A

### ARE ADDITIONAL PERSONNEL REQUIRED?
- ☐ Yes, -- --
- ☒ No

### IS THIS ITEM ALLOCATED IN THE BUDGET?
- ☒ Yes  ☐ No

### IS A BUDGET TRANSFER REQUIRED?
- ☐ Yes  ☒ No

---

### BOARD BELOW FOR CLERK’S USE

#### BOARD ACTION:
- ☐ Approved
- ☐ Approved as amended
- ☐ Adopted
- ☐ Adopted as amended
- ☐ Denied
- ☐ Other
- ☐ No Action Taken

- ☐ Set public hearing
  For: ______________________

- ☐ Direction to: ________________

- ☐ Referred to: ________________

- ☐ Continued to: ________________

- ☐ Authorization given to: ___

- Resolution 2016- _____________
- Agreement 2016- _____________
- Ordinance _________________

**Vote:**
- Ayes:
- Noes:
- Abstain:
- Absent:
- ☐ By Consensus

### COMMENTS:

---

**CLERK TO THE BOARD**

**DATE**
Sierra County

Information Technology Policy

March, 2016
# Table of Contents

Mission Statement ...................................................................................................... 3

Security Policy and Procedure ................................................................................... 3

Electronic Media and Use Policy ............................................................................... 4

Email Retention ......................................................................................................... 7

Litigation Holds ......................................................................................................... 9

California Public Records Act (PRA) Requests ...................................................... 10

New Employee Network Access ............................................................................. 11

Terminating Employee Access ................................................................................ 11

Requesting Assistance from IS Department ............................................................ 11

Virtual Private Network (VPN) Access ................................................................... 12

Personal Devices ...................................................................................................... 12

Portable Devices ...................................................................................................... 12

Social Media Policy ................................................................................................. 13

Software Management Plan ..................................................................................... 13

Electronic Data Disposal .......................................................................................... 13

Viruses ..................................................................................................................... 14
Mission Statement

The Information Systems Department is responsible for the data, voice and video systems operated by the various functions of Sierra County government. It is the responsibility of this Department to ensure that these systems operate at maximum efficiency and are available to every location at all times when needed.

As time passes, data processing, voice and video communication in real time are merging into a unified system. Computers are more like voice and video communication systems and phone have become computers.

This Department has accepted the responsibility of keeping the information systems operating at all times. To deliver on this responsibility:

1. We will acquire and place into operation the best technology available that is compatible with the resources of county government and with the culture and needs of Sierra County's citizens and the government employees who provide services to the citizens.

2. We will maintain the systems so they function and to ensure that each workstation is supplied with the high quality voice and data processing and internet access at all times during the working day. The working day is that time frame that the workstation is actively manned. If the working day is around the clock, it is the responsibility to ensure continuous operation 24/7.

3. We will 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.

4. We will protect these systems from injury, whether such injury originates internally or externally. We will strive to protect both the hardware and the software.

5. We will set priorities as to the use of departmental resources which priorities will follow the direction of the county's legislative body and will direct the resources toward benefiting the greatest number for the greatest good. Emergency services will always receive the highest priority.

Security Policy and Procedure

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

Some workstations may, with prior approval of the IS Manager, be allowed to have department-specific applications as long as these do not cause conflicts.

Passwords, once issued, shall not be shared by employees. If a Department has the need to access the computer of an absent employee, the Department Manager must make request to the IS Manager or the IS Assistant Manager for access. No employees, other than a Department
Manager or assigned IS staff, shall be provided access to another employees’ account. Upon return of the effected employee, the IS Manager shall issue a new password.

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

Only specific workstations and password-identified persons are to be allowed on each department’s shared files located on the server.

The doors to the two computer rooms are to remain locked except when the IS Technicians or other 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 shall be loaded onto each workstation by IS staff.

All Virtual Private Networks (VPN) are to have their own point of contact security. VPN access is permitted only after the VPN Use Agreement has been read and signed by the requesting employee, submitted by the employees' Department Manager and approved by the IS Manager.

The IS Technicians are authorized to remove any non-approved applications, including screen savers, from any workstation connected to the County network.

All servers are backed up on a set schedule. Back-up tapes are distributed and stored in a fire-proof container.

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

The Information Systems Manager is responsible for the enforcement and interpretation of this Policy.

As technology and safety requirements change, this Policy may be updated by the Information Systems Department without expressed written approval of the Board of Supervisors.

**Electronic Media and Use Policy**

The purpose of this policy is to establish guidelines for proper use of all forms of the County’s electronic media. The term “network” includes all electronic systems developed by and used by Sierra County government. This includes the county web site, the internet, all local networks including telephones and facsimile transmissions.

The network, including the email component, is for County government business only. Use of the Sierra County data processing network, including the high-speed internet, is limited to county departments and employees only. Employee use of any County electronic media system is not private, and employees using these systems should not expect their communications to be private. Employees should be aware that Internet activity is logged and monitored on an
individual basis. Employees should also be aware that any communication or internet activity, including but not limited to email, voicemail and internet browser history, may be considered a public record subject to disclosure under California law. Misuse of the network has the same consequences as the misuse of any government property.

Use Policy:

1. The Sierra County electronic media systems are made available to employees for the purpose of providing an effective method to communicate, increase productivity, perform research, and obtain information that will assist in performing job-related tasks.

2. Employees shall use good judgment at all times when using the Internet or other electronic media. Electronic media shall be used only to send courteous, professional, and business-like communications.

3. Electronic media communications (such as email) should always be treated as written memos which may remain on file in various locations and be read by persons other than the sender and recipient. The County may save such communications even though it appears they have been deleted.

4. The County has the capability to access, monitor, review, and copy or disclose any activity on the County network; and the County reserves the right to do so for any proper County purpose. The use of security measures (such as individual passwords) or deletion of electronic media communications (such as deletion of email messages by users) does not affect the County’s ability or right to access, review, copy or disclose such communications under appropriate circumstances. Employees’ use of electronic media is consent to such action by the County.

5. Users of County email and communications systems should be aware that (1) their email/communications are not personal and private, (2) their email/communications may be (but are not necessarily) saved for future reference and (3) their email/communications may be seen by persons other than the original addressee.

6. Knowledge of passwords, loopholes, or other means of gaining access to network, data, communication, application, server, document, website, device, and associated computer security systems will not be used to damage computing information or resources, gain unauthorized access to information and resources, or otherwise make use of information or resources for which proper authorization has not been given. Accessing data on the County computer systems unless expressly authorized is strictly prohibited.

Incidental Personal Use:

Electronic communication resources are provided by the County to facilitate the performance of County work. Under no circumstances other than that which is expressly permitted, should an employee use any County resources for personal use.
Incidental personal use is permitted, so long as employee use of the systems are 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), and only so long as the Department Head determines that the operation of the Department is not being compromised or disrupted.

Incidental personal use should be minimal, and should not:

1. Interfere with the County’s operation of the data processing network;
2. Interfere with the user’s employment or other obligations to the County, or
3. Incurring costs other than de minimis in nature.

Incidental use of the County’s data processing network should clearly indicate that the use is personal. Users of electronic communication resources will not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the County unless appropriately authorized to do so. The County is not responsible for any loss or damage incurred by an individual as a result of personal use of the County’s data processing network.

Prohibited Activities:

Electronic media shall not be used in any manner in violation of the law or County rules, policies or procedures. Electronic media shall in no manner be used for any improper, illegal, offensive or harassing purpose.

Activities prohibited by this policy include, but are not limited to, the following:

1. Unauthorized access or removal (file review, transmittal, removal, copying) of any material or communication in violation of any federal, state or local law, ordinance or regulation. Unauthorized employees accessing data will be subject to personnel disciplinary action, up to and including, termination.

2. 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).

3. Misrepresentation of an employee’s true identity.

4. Attempting unauthorized access to data or breaking into any County or non-County network.

5. Any action intended to accomplish or assist in unauthorized access to computer systems.

6. Unauthorized or improper downloading, accessing or transmittal of information, documents or software, including any acts that infringe copyright. Employees shall use software only in compliance with license agreements and as authorized by the Information Systems Manager.
7. Any action which causes the County to incur a fee for which there has not been prior approval.

8. Use of a security code or password other than as authorized.

9. Disclosing your password to anyone other than IS staff members for any purpose.

10. Any use of the County electronic media for the purpose of individual private remuneration.

11. Any unauthorized use of the County resources in a way that suggests County endorsement of communication for personal use.

12. **Personal use of a County cell phone.**

13. **Unauthorized employee access of email exchange server during non-business hours.**

14. Transmittal of unauthorized broadcast communications or solicitations, such as mass email transmittals. All broadcast or solicitation messages must be approved in advance by the Department’s Manager and/or the Information Systems Manager.

15. **Engaging in recreational 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.

16. **Storage of county data in a cloud environment.**

**Email Retention**

Electronic mail has become a ubiquitous service that greatly enhances communication, both internally within Departments of the County of Sierra, and externally to clients, taxpayers and the public at large. All emails transmitted or received through the County email system are subject to being read by the County management and may be subject to being disclosed as public records. It is the intent of this policy to limit the retention and storage of emails to those necessary for the County’s business or required by law.

This policy establishes the default retention period for email retained within the County computer network. It also confirms the roles and responsibilities for implementation, including the management of litigation holds.

This retention policy applies to all users and account holders of the County of Sierra email system and all email sent or received using the County email system.

**Transitory Messages**
Most email records are created primarily for routine communication or information exchange between departments and offices within the County of Sierra and are considered transitory messages that are not intended to nor needed to be retained as permanent records of the County.

Such emails should be:
Read and retained on the active server for no longer than the default retention period (defined below).

Some examples of transitory messages are:

- Notices about meetings
- Internal requests for information
- Announcements, etc.
- Informal communications

**Messages to be Retained**

When the contents of an email exhibits one or more of the following characteristics, it may, in the judgment of one or more of the parties to the email, be appropriate to retain same as a permanent record;

Each County Department shall develop a retention policy, identifying specific record retention practices as required by law.

Since email systems are not designed to be records retention or document management systems, email to be maintained as permanent records should be saved in accordance with the retention policy established by Department. The decision as to whether a specific message should be retained as a permanent record will be set forth in the Departments adopted retention policy. Questions regarding retention policies are to be answered by the Department Head and/or County Counsel.

**Default Retention Period**

The County of Sierra email system will be configured to automatically delete messages retained for more than six (6) months on the active email server. This auto-delete policy applies to emails located within the inbox folder, sent file folder and delete file folder stored on the active email server.

**Backup Files**

Backup discs of County of Sierra email files will be kept for no more than three (3) weeks. These backups are for system restoration and disaster recovery purposes, and are not designed to facilitate retrieval of deleted messages.
Litigation Holds

When litigation involving Sierra County or its employees is pending or anticipated the law imposes a duty upon the County to preserve all documents and records that pertain to the issues. This includes all relevant emails.

Upon receiving any indication of potential litigation, a department head should immediately issue a litigation hold and refer the matter to County Counsel. The litigation hold shall be directed to all persons having access to and/or control of the information. Where a litigation hold is to be directed to a person who is separated or otherwise unavailable, the Department Head and/or County Counsel shall instruct the Information Systems Department and any other necessary personnel on the existence of the hold and the necessary steps to preserve the information. Department Head shall be responsible to provide the IS Department a written list outlining specific employees with access to and/or control of the litigation.

The hold shall indicate the subject matter covered by the litigation hold, state that the hold shall be in effect until expressly revoked in writing, and shall instruct those parties on the step reasonably necessary to ensure that all relevant information (including but not limited to documents, drafts, emails, recordings, notes and other materials) are adequately preserved from either manual or automatic destruction. If anyone other than County Counsel is issuing the litigation hold, they need to confer with Counsel to ensure there is a clear understanding of all the issues relevant to the litigation or potential litigation.

A litigation hold directive may be issued by the County Counsel, outside counsel retained to represent the County, the Risk Manager, or a Department Head and must be issued to all departments and employees having access to and/or control of the information.

A litigation hold directive overrides this email retention policy, as well as any records retention schedules that may have otherwise called for the transfer, disposal or destruction of relevant documents, until the hold has been cleared.

IS Staff shall be responsible for saving all email communications. Employees’ shall be responsible for saving all documents.

Email and accounts of separated employees that have been placed on litigation hold status must be maintained by the Information Systems Department until the hold is released.

No employee who has received a litigation hold directive shall alter or delete an electronic record that falls within the scope of that hold. Mark-ups, notes and drafts will be considered separate documents in the event of a litigation hold. Those employees are required to provide access to or copies of any electronic records that they have downloaded and saved, or moved to some other storage account or devise. Questions about the scope of a litigation hold shall be directed to County Counsel.

Roles and Responsibilities
The Information Systems Department will:

1. Provide all County employees with the required helpdesk support.

2. Manage server implementations of litigation holds that are issued by County Counsel.

3. Suspend automatic deletion processes, as necessary to preserve specific electronic messages, records and information that fall within the scope of the litigation hold, and that reside on active servers.

Department Heads shall be responsible for creating and providing records retention guidance to all staff within their respective departments. The policy shall establish clear policies as to the types of records and emails that will be saved, as well as how, where and for how long they are saved. The guidance provided must be in accordance with this policy.

Originators and custodians of electronic messages, records, and information are to be retained pursuant to Departments’ adopted retention policy:

- Appropriately identifying and retaining such records in accordance with this policy.
- Seeking assistance from their respective Department Head when unsure about how to categorize specific types of messages.

County employees who have been notified by either County Counsel or their Department Head of a litigation hold shall be responsible for preserving all messages, records and information that falls within the scope of the hold that they have downloaded and/or stored on the County computer network.

**California Public Records Act (PRA) Requests**

Access to information concerning the conduct of the people’s business is a fundamental and necessary right of every person in this state. Records of the County of Sierra which are not exempt from disclosure are available for inspection and copying in accordance with the California Public Records Act upon a request that reasonably describes and identifiable record or records.

The California Public Records Act is found in the California Government Code, beginning at Section 6250. Records subject to inspection and copying include any writings, meaning any handwriting, typewriting, printing, photostating, photographing, and every other means of recording upon any form of communication or representation, including information available in an electronic format. (Gov. Code Sec. 6252(f) and 6253.9)

The County of Sierra does not maintain a centralized record keeping system. County department, agencies, commissions and committees are located at various public facilities within the County.

Requests to inspect and copy public records, which are not otherwise immediately available to the public, should be made directly to the responsible department or agency head, commission or committee, or to his or her designee. County employees have an obligation to assist members of
the public who are not sure what type of record contains the information they are seeking, including which Department should be contacted.

Records shall be made promptly available for inspection, and for copying within ten (10) calendar days after receipt of request. In unusual circumstances, the ten (10) days may be extended by written notice from the department or agency head, commission or committee, or from his or her designee, for no more than an additional fourteen (14) days as provided by law.

Within five (5) days of receiving a Public Records Act Request, it is the responsibility of the department or Department Manager, commission or committee, or his or her designee, to contact County Counsel if any question exists whether any record, or portion of any record, is exempt from disclosure. The County Counsel shall be responsible for providing advice to the department, agency, commission or committee, and for assisting the department, agency, commission or committee in drafting a written response if an exemption is claimed.

A fee for copies of public records may be charged which covers the direct costs of duplication as determined by County Fee Schedule.

**New Employee Network Access**

Department managers, or authorized personnel, shall request new employee access to 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 of the form, IS staff shall provide copy to the Auditor’s Office. It is the responsibility of the Department Manager to maintain the ReadyDesk ticket for new employee access.

**Terminating Employee Access**

IS technicians shall not terminate employee access to the county network until a *Termination Request Form* has been submitted by the employees’ Department Manager. Department Managers shall submit the Termination Request to the IS Manager. In the event the IS Manager is unavailable, the Department Manager shall submit the request directly to an IS Technician. Upon receipt of the Termination Request, IS technicians will review the form and terminate access as noted.

If a Department Manager is dismissing an employee, the effected employees’ Department Manager, or authorized personnel, shall notify the IS Manager prior to notifying the effected employee of the termination to ensure protection of county property. IS technicians shall immediately terminate access and notify the effected Department Manager, or authorized representative, when network access has been severed.

**Requesting Assistance from IS Department**

To request the assistance of the IS Department, employees must submit a ReadyDesk Ticket. The sole exception to this policy is when a Department Manager has provided a *Termination Request Form* to the IS Manager or IS Technician.
A *ReadyDesk User Guide* has been created for use and shall be supplied to all new employees by IS Department on first day of employment.

**Virtual Private Network (VPN) Access**

This policy is intended to clarify the requirements of being provided access to County computer networks using a Virtual Private Network (VPN).

No employee shall be provided with VPN access without specific written consent from their Department Head and Information Systems Manager. Department Head shall be 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 Manager, IS staff will provide employee virtual access to the network. No employee shall access the county computer network other than through the use of a county-owned and county-monitored computer. If requesting office does not have a county-owned and county-monitored computer, contact the IS department to see if one is available for use. Offices that have county-owned and county-monitored computers shall ensure those computers are plugged into the county network bi-monthly to receive security and software upgrades.

Employees accessing the county computer network using VPN access shall abide all applicable privacy laws and maintain confidentiality at all times.

**Personal Devices**

With the exception of elected, appointed and mid-management positions, no personal devices not limited to, iPods, iPads, laptops and personal computers shall be connected to the County network. Personal devices, however, may still connect to those wi-fi networks designated by the County for public access.

**Portable Devices**

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

- Employee name
- Date assigned
- Date returned
Social Media Policy

The County endorses the secure use of approved social media technology to enhance communication; collaboration and information exchange; streamline processes; and foster productivity improvements for safety sensitive departments. However, the technology must not compromise data confidentiality and integrity. Departments use of social media technology shall conform to the policies, protocols and procedures contained, or referenced, herein.

Social media uses many technologies and forms, including social-networking, blogs, wikis, photo-sharing, podcast, social bookmarking, mash-ups, widgets, virtual worlds, microblogs, Really Simple Syndication (RSS) and more. Not all forms of social media may be appropriate for use by County Departments.

Social media applications used by County offices shall be approved by the Board of Supervisors prior to use.

For information on which social media platforms have been approved for use, contact IS Administrator.

Software Management Plan

To prevent copyright infringement and promote good software management practices, Sierra County IS Department shall maintain a software management program. IS Technicians shall document license numbers, serial numbers, date of purchase and log warranty expiration date for all purchased software. IS Administrative Assistant shall, with assistance from IS Manager, track license expiration and ensure timely renewal of all software license agreements.

Electronic Data Disposal

All computer systems (PC’s, Laptops), electronic devises and electronic media must be properly cleansed of sensitive data and software before being transferred outside of County of Sierra either as surplus property, broken electronic devices, recycled or trash.

Computer hard-drives and portable devices (thumb-drives, portable hard-drives) that are no longer used by County employees must be sanitized. Non-rewritable media, such as CD’s or non-usable hard drives, must be physically destroyed.

The primary responsibility for sanitizing computer systems, electronic devises and media rests with the IS Department. County employees shall surrender all unused electronic devices to the IS Department for disposal.

Background
A large volume of electronic data is stored on computer systems and electronic media throughout the County. Much of this data consists of confidential and sensitive information, including financial data, personnel records, property characteristics and medical records. The County of Sierra is mandated by several federal and state laws that set forth the responsibilities for protecting this information, including the Federal Privacy Act and the Health Insurance Portability and Accountability Act (HIPPA). In addition, copyright laws and software license agreements protect vendor rights regarding the use of software.

Unauthorized disclosure of sensitive information may subject the County of Sierra to legal liability, negative publicity and monetary penalties and harm the rights of employees or members of the public. All sensitive information and licensed software must be properly removed when disposing of computer systems with hard drives, PDA's and removable media, such as, but not limited to CDs, DVDs, USB drives, Zip discs, diskettes, tapes, smart cards and thumb drives.

The method of destruction of the media shall be made by physical force by IS staff, with the Information Systems Manager a witness to the physical destruction.

**Procedures**

Information Systems Department staff is responsible for the disposition of surplus computer systems and electronic devises. All surplus computer systems and electronic devises that become the responsibility of the IS Department shall be logged onto the *Electronic Data Disposal Verification* log maintained by the Information Systems Manager in cooperation with IS Staff.

Disposal of computer systems and media shall comply with all environmental regulations.

**Viruses**

If you discover, or fear, that a virus has infected your computer and/or device, do not send any messages and do not use the computer. Contact the Information Systems Manager or the Assistant IS Manager by phone. IS Technicians will scan the effected device, remove the virus and return the device to the effected employee.