

**BEFORE THE BOARD OF COUNTY COMMISSIONERS
FOR COLUMBIA COUNTY, OREGON**

In the Matter of Updating the Columbia County)
Electronic Systems and Equipment Use (IT) Policy) **ORDER NO. 11-2015**
_____)


WHEREAS, the IT Policy has been updated to reflect current practice and industry best practices, where feasible;

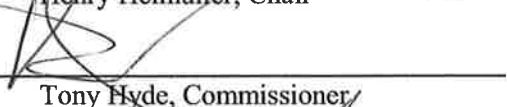
NOW, THEREFORE, IT IS HEREBY ORDERED that the Columbia County Electronic Systems and Equipment Use (IT) Policy as shown in Exhibit "A" which is attached hereto and incorporated herein by this reference be adopted; and

IT IS HEREBY FURTHER ORDERED that the Columbia County Electronic Systems and Equipment Use (IT) Policy shall become effective immediately.

DATED this 1st day of April, 2015.

**BOARD OF COUNTY COMMISSIONERS
FOR COLUMBIA COUNTY, OREGON**

By: 
Henry Heimuller, Chair

By: 
Tony Hyde, Commissioner

By: 
Earl Fisher, Commissioner

Approved as to form

By: 
Office of County Counsel

Exhibit "A"

COLUMBIA COUNTY, OREGON

Electronic Systems and Equipment Use (IT) Policy

SECTION 1. PURPOSE

This Policy establishes procedures and guidelines that specify who owns and controls the information within Columbia County's Electronic Information Processing System ("System"), the County's right of access to the information contained in the System, and the use of the system, associated network, software and equipment. This Policy extends to personal devices if County information is located on those devices or if they are used to access the County system.

A further purpose is to ensure that electronic records and communications are maintained and stored according to Oregon Public Records law.

SECTION 2. SCOPE

This Policy applies to all County employees and others ("Users") who have access (direct or through any type of remote access solution) to the System. The System includes all computer devices (whether network or stand alone) software and hardware (workstations, laptops, memory devices, storage devices and storage media, etc.), telephones, mobile devices of any type, cellular-based communications devices that access the County network (whether these devices are owned by the County or by other agency or by employees personally), voice mail, faxes, printers, county maintained websites and County maintained social network sites as well as any web based software programs or systems utilized by the County for data purposes. For purposes of this Policy, an electronic record or communication includes any data or information in any form processed or stored within the System whether generated directly or indirectly.

Where any section, subsection, sentence, clause, or phrase of this Policy is found to conflict with any state or federal law or administrative rule, the terms of such laws or rules shall prevail.

SECTION 3. POLICY

The System is a County resource and tool for assisting in the conduct of County business. Unless otherwise specified by formal written agreement, all programs, documents, and data generated, processed, and/or stored on the System are County property. Use of the System shall be conducted in accordance with this Policy. Other policies, such as the County Personnel Rules, may also apply to subjects of this Policy.

SECTION 4. BACKUP OF ELECTRONIC FILES

Information Technology ("IT") staff periodically backs up or contracts for the backup of County data including e-mail. These back-ups are not intended for storage of documents, but are solely for the purpose of restoring needed, active files in the event of accidental deletion or data loss. Users are not

to rely on these back-ups as a document retention mechanism, as the in-house backup media is routinely recycled every 30 days. Local hard drives on personal computers (PCs) are not backed up and should not be used for storage of electronic records. IT will not expend any effort, beyond a basic initial attempt, to restore data from a damaged hard drive. IT is not responsible for transferring data stored on local hard drives if that data should and could have been stored on the network system. Data stored on local hard drives will be lost if the hard drives fail.

SECTION 5. COMPUTER NETWORK SECURITY GUIDELINES

Network security, both internal and external, is vital to the County. Security breaches could lead to loss of network access (resulting in a substantial loss of productivity), release of private/confidential information (of employees or of the public), liability to the County for data loss and/or damage to the County's credibility and reputation as well as causing the individuals involved and/or the County itself to be in violation of State or Federal law related to the various systems used.

Users are responsible for following reasonable security practices regarding System physical access, System configuration and network rights.

A. System physical access

Physical access controls protect critical information systems. All computer equipment will be inventoried and tracked by IT. If equipment is moved or re-assigned from its original placement, notification must be sent to IT.

All critical System level components will be stored in a location with restricted access controlled by key or security door. All employees with access to secured locations should be strictly controlled through Facilities. All equipment in storage should be locked with access restricted to only administrators. Access to secured locations, including stored equipment, is strictly off limits unless accompanied and supervised by authorized personnel.

Access to IT secured locations by outside services providers, such as electricians, carrier-based technicians (voice and data), hardware and software technicians, and building maintenance personnel should be supervised by authorized personnel at all times. All wiring closets housing network or other related equipment should be locked at all times.

All access authorization for employees terminated or who give their notice of intention to leave shall be revoked or disabled upon separation from the County or earlier if deemed in the County's best interests.

Users will log out of the network and turn off their computers when not in use overnight and over weekend periods, unless there is a pre-authorized business purpose for leaving the computer on (such as computers in the Sheriff's Office that require 24 hour access).

Users will follow reasonable guidelines for physically securing work areas during work hours and off-hours. Each department is responsible for establishing procedures regarding closing and locking appropriate doors.

Users will identify "high risk" locations to IT. A work area in which a workstation cannot be effectively secured for County-only utilization, or is expressly configured for access by the general

public, is considered to be "high risk."

No member of the general public should be provided access to County equipment unless that equipment has been configured and approved by IT specifically for public access.

To ensure network security, no User will connect any device to the County network (including wireless) without prior approval from IT.

Users will report any concern regarding unauthorized utilization or suspected tampering of any County system device to IT immediately.

B. Network Rights

A User profile is established for each individual at the time network rights are established. This profile will limit the User's session to only the information resources required for performing his or her job. If the User feels he or she is constrained by rights afforded through an existing profile, a request for review from the User's supervisor should be placed with IT. Additional access shall not be achieved through sharing the network rights of others, nor should it be explored through attempting to access systems on an unauthorized basis.

New user accounts will be established by IT only upon receipt of the properly completed form by the relevant department supervisor. When a user moves from one department to another department within the County, IT shall delete the rights from the user for the prior department and set up the account with new access rights appropriate to the new department.

Network passwords are utilized as a key element of the System security strategy. Passwords are required of all Users. System requirements as defined by IT for minimum password length, password renewal, and password reuse apply to all Users of the System. System Users should protect their passwords and change them immediately if the password is compromised. Users may be required to share their passwords with their supervisor. Periodic password changes, with limitations on password reuse, are enforced as a matter of network security. IT may require that passwords that do not meet minimum security requirements be changed immediately.

C. Devices that Operate off the Network (including portable devices and removable media)

All computing resources and information media must be secured to prevent compromise of confidentiality or integrity. Password protection shall be employed on all laptops/notebooks, mobile devices and other similar devices carried into the field by County employees. Devices that do not support password protection should not be used to store County data. Users assigned portable devices are responsible for ensuring the physical security of those devices. Devices should not be left in vehicles or in any other unsecured location. Users may be required and shall be prepared to provide an inventory of data which existed on any device that is lost/stolen/damaged.

Special care must be taken to ensure that information is not compromised when using mobile computing devices or media including laptops/netbooks and mobile phones, flash drives, floppy diskettes, CDs, DVDs or removable hard drives. This includes precautions to prevent potential compromise through loss or theft of the device.

There is risk of disclosure of sensitive information through careless disposal or re-use of equipment. Processes which are applicable to a department's work flow shall be established in each department

to minimize this risk. Storage devices such as hard disk drives and other media (e.g. tapes, diskettes, CDs, DVDs, flash drives, digital copiers or other devices that store information) or paper containing sensitive information must be physically destroyed or securely overwritten to prevent the unauthorized disclosure of sensitive information.

D. Remote or Online Access to System

Employees may remotely access their assigned voice mail boxes at any time, except that FLSA non-exempt employees may only access their assigned voice mail boxes during regular working hours or when pre-authorized by their supervisor for specific after hours access.

All references to remote or online access in this section refer to any access to County data from a non-County access point and/or outside of regular working hours.

Users requesting remote or online access to any County data system, including email, must receive approval from their manager or supervisor, Users who are granted access are responsible for complying with the following:

- Users in possession of remote access voice mail numbers or IP addresses/URLs are prohibited from sharing this information with unauthorized users.
- Users are not permitted to “save” remote or online access usernames and passwords in the workstation’s remote access client application. Users must enter the username and password at the beginning of each remote or online access attempt.
- All remote access lines must be protected with an encrypted username and password.
- All IP addresses will be captured and be included in the logging information.
- All hosts available to end-users via remote access will be configured to log-off upon a loss of communication with the virtual terminal.
- Users will immediately terminate a remote or online session when it is no longer in use.

Remote or online access is not permitted for personal use.

IT will provide no technical support for personal devices or home computer equipment related to remote or online access. Non-exempt employees will be granted remote or online access only when approved by a supervisor and must appropriately record all time worked accessing the System remotely, which can be matched to logged activity. Remote access will not be supported during any time in which IT is engaged in other vital System work and will be ended whenever needed for the health of the System.

Remote or online access capabilities are assigned to specific individuals and are non-transferable between Users. Users are never to share their login password with anyone. Users are not permitted to use another individual’s login ID and password.

All users utilizing remote or online access are required to maintain current, valid, and updated anti-virus software utilizing the latest available virus definitions and a firewall between the device and the Internet. For home users, a hardware firewall is strongly recommended, however, a broadband router and a software firewall is acceptable. Proper security configuration of personal equipment used to remotely access the County System is the responsibility of the User. The County may audit any equipment used for remote access to the County’s network. If the personal device is not found to meet County requirements, remote access privileges will be revoked. This includes personal

equipment under the following guidelines:

- Such audits are performed strictly to ensure compliance with this policy.
- Audits will not be performed without at least 24 hours notice.
- Audits will only be performed in the company of the user

Audits will be performed to:

- Verify the existence and operation of Anti-Virus software
- Verify the existence and operation of a Firewall (hardware or software)
- Verify that no active virus or malware is found on the system by performing a virus and/or malware scan.

If a virus is discovered by IT on personal equipment used for remote or online access to any County system, a **basic** attempt by IT will be made at removal. Should the virus not be removed or doubt exists about the device's security, it will be the user's responsibility to remove the virus, at their expense. Remote access will be disabled until the system is verified virus-free. Remote access users are expected to cooperate fully with IT or immediately forfeit remote access rights.

Any User who violates any provision of this Policy will immediately have remote access privileges revoked and may be subject to disciplinary action.

External entities, such as state/local agencies, County business partners, or vendors, may request access to the County's System. These requests will be granted only on a very limited basis and only at the discretion of IT. Benefit to the County must be shown, there must be no other reasonable alternative method to gain access and the external entity must comply with all County security requirements.

E. Unauthorized Use of Utilities and Network Tools

Many sophisticated system monitoring and diagnostic tools are readily available through the Internet. Implementation of any type of these tools, including keyboard capture, network diagnostic, scanning, "sniffing", remote workstation access, or port mapping tool by Users is prohibited. Managers should contact IT if there is a requirement to use these devices to conduct County business.

F. System Configuration

Careful control of access points to the network is vital to System security. No User shall install, or allow an outside service provider to install any software or hardware solution that allows remote access or remote control of a device within the County network. No User shall utilize any unauthorized software package or service to gain access to a device outside the County network. A network connected device configured with a remote access or remote control software represents a significant security exposure to the entire network. IT will work with the User to assure that required needs are met with a configuration that is consistent with System security requirements.

A firewall is maintained to separate the County network from the Internet. Many web-based services offered by outside agencies, for communicating and transferring data, require modifications to the firewall. Every modification constitutes a compromise in network security. IT will assess requests for access through the firewall on a case by case basis through a formal request process.

No User should attempt to modify their desktop/other device operating system or software

applications installed on the System. This includes the use of registry editors, any type of disk management software, menu, or other utility whether included in the standard operating system or not. Users should not experiment with their device operating system configurations.

No User should install or download any software or program onto the System, this includes County equipment not connected to the County network. In general, IT is solely responsible for installation and configuration of software on devices and the System. Some specialized circumstances warrant Users installing and maintaining their own applications provided they do so by specific agreement with IT. Users should consult with IT prior to responding to any prompt from any source to upgrade standard components on County devices unless they have otherwise been directed to accept these prompts related to certain types of commonly used software resident on the System.

IT relies on standard configurations when restoring systems after component failures. IT will not restore any custom configurations implemented by end users.

Users shall not disable or modify the network security software placed on their system including anti-virus software. Users connecting to the network are obligated to participate in distributed updates of their systems.

G. Software and Hardware

No unauthorized software or hardware shall reside on County computers. IT will remove any unauthorized hardware or software found on an User's computer. Notice may or may not be given to the manager and User after removal.

Any commercial software shall be purchased through an authorized vendor or otherwise lawfully obtained. The software license and transfer media shall be stored in a secure location in IT.

Standard software is that which is common to all County computers and authorized by IT. Standard hardware is hardware authorized by IT.

All software, hardware and peripheral items are to be purchased with the approval of or by IT and not by the individual user or departments. Requests for nonstandard hardware and/or software shall be approved by IT.

To ensure proper software licensing and inventory control, IT will periodically audit installed hardware and software on each County workstation.

No personal equipment of any type may be attached to the County System without prior approval of IT.

Unless otherwise allowed under the software license and for purposes of backup or archival as determined by IT, software owned by the County or installed on County computers are covered by copyright laws and shall not be copied, duplicated or installed on any other computer. This applies to software and to manuals.

No software may be downloaded or installed onto a County computer without the approval of IT.

H. Software Licensing Policy

All programs, documents, and data generated, processed, and/or stored on the System are County property, unless otherwise specified by a license agreement. The County licenses the use of copies of computer software from a variety of outside companies. The County does not own the copyright to this software or its related documentation. The County, except for copies for backup purposes or unless expressly authorized by the copyright owner(s), does not have the right to reproduce it for use on more than the authorized number of computers or network.

Users are not permitted to copy any software or program on or connected to the System.

County employees learning of any misuse of software or related documentation within the County should notify IT. According to the U.S. and Canadian Copyright law, unauthorized reproduction of software is a federal offense. Offenders can be subject to civil damages of as much as US\$100,000 per title copied, and criminal penalties, including fines (up to US\$250,000 per work copied, CN\$1,000,000) and imprisonment (up to 5 years per title copied).

I. Electronic and Physical Destruction of Media

IT shall sanitize (by overwriting at least three times) or physically destroy electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). IT shall maintain written documentation of the steps taken to sanitize or destroy electronic media which is sanitized or destroyed by IT. Departments with access to the Criminal Justice Information system (CJIS) shall also document steps taken by Department personnel to destroy or sanitize electronic media and also ensure the sanitization or destruction is witnessed or carried out by authorized personnel. All electronic media contained in hard drives of any type must be sent to IT for disposal. Departments may dispose of removable media such as CDs, DVDs, USB flash drives, only if they follow the procedures outlined above to do so.

J. Technical Support Procedures

The objective of user support is to ensure that information technology tools are in place, function and provide access to required information. User support will generally be provided between the hours of 7:00 am and 5:00 pm Monday through Friday (contingent upon availability of limited staff). Access to IT staff for after hours emergencies is also available for departments that operate outside these hours, such as the Jail and Sheriff's Office. This access will be established on an individual basis.

Requests for support shall be made to IT by e-mail to mailbox "Computers". In the event that the County e-mail system is down, contact IT at Ext. 7231. Users must clearly identify the user, department, equipment involved and the problem experienced.

Prior to making contact with IT:

- Users should shut down the computer/device, wait 20 seconds and restart to see if this solves the problem.
- If unable to print, users should save the document, and follow shutdown instructions as above.
- If still unable to print, users should power off the printer, wait 20 seconds and restart the printer.

Response to computer requests is based first on availability of IT staff, then on the degree of the

problem balanced with all other existing problems. The nature of the problem will also be considered in evaluating priorities. IT will respond first to highly critical problems; second to critical problems affecting many individuals; third to critical problems affecting an individual, and to annoying problems as time permits. Priority will be given to hardware and software that supports the network and multiple users and to existing applications.

When a User or department feels a problem is not being addressed appropriately, the User or manager should contact the IT Director to discuss appropriate resolution.

Employees shall not move their computers or other peripheral equipment without notifying IT of the move in advance. IT will not provide support for moving system equipment unless the department has scheduled the move at least one week in advance.

K. User Monitoring & Inappropriate Behavior

Use of the County system may be monitored at any time for any reason by IT. IT staff may become aware of inappropriate behavior during the course of monitoring the system, providing routine maintenance for computers, reviewing blocked e-mails, or monitoring users under the direction of the IT director. If IT staff become aware of a problem they will notify the IT Director who will work directly with the affected department and/or Human Resources to address the problem appropriately.

Any manager wishing access to staff e-mails, Internet access or other logs shall make the request of the IT Director, who will respond appropriately in coordination with Human Resources.

L. Internet Access

Managers are responsible for identifying staff that require Internet access and to ensure that staff use the Internet appropriately. All Internet access is logged and may be monitored at any time. If IT becomes aware of Internet access problems, the IT Director will notify the manager, who is responsible for taking appropriate action.

Users are not to download any software of any type off the Internet without IT's prior approval.

M. County Web Site and Social Media

The purpose of the County web site is to provide accurate, unbiased and useful information to the public about County services and programs and the community.

The County web site will have a consistent look and feel for all departments. IT will be responsible for developing the web structure and the general look and feel. Departments will be responsible for content. The site will meet ADA standards.

The County web site will balance delivery speed with acceptable aesthetics. The site will be viewable with commonly available access speeds in the area. Features such as video, graphics, pictures, animation, and music that require high throughput will be kept to a minimum and used only to provide meaningful content or to significantly improve aesthetics.

The County web site may provide links to government and other partners of the County but will not provide links and advertisements for commercial enterprises.

All departments are responsible for the content of their web page. IT will provide guidance on the

required structure for the web design.

See the separate Policy on Social Media for procedures by which departments may develop and use social media to conduct County business.

N. County Online Data/Web Based Applications

The County utilizes many different web based applications including for email, backup, payroll, HRIS, Transit, etc. The rules regarding use of and access to these web based systems is the same as if the data or application were stored in house. Employees may not use access to web based system to violate any section of this or other Policies. Employees may not use online data storage capacity (such as Google Drive) to store County documents. All rules regarding confidentiality, public retention, etc. must be complied with when utilizing web based systems.

SECTION 6. HOME USE AND USE OF PERSONAL EQUIPMENT

Users may not use home computers, printers, laptops, or any other devices for County business at work. County information stored and managed on a computer must be managed as part of the County information infrastructure, be secure, and be managed to meet County requirements. Exceptions to this rule require IT Director and department head approval.

If a User chooses to perform County work on any non County equipment (NCE) away from work, the User will:

- Accept total responsibility for all operations of the NCE.
- Understand that the County will not supply any support or accept any liability for the NCE.
- Ensure that any data, information, or documents developed for County business will be done using tools that are compatible with the County standards.
- Agree that the use of the NCE is strictly for personal convenience.
- Keep only temporary copies of County work on the NCE. Master copies of all information will be kept on the County System.
- Check any information loaded from a removable media (CD, DVD, flash drive, etc) for viruses prior to downloading any information to the County System.
- Obtain prior permission from the supervisor/department head/IT.
- Not use a personal e-mail address in place of County e-mail.
- Observe any confidential or privacy requirements of the department has for the information.
- Not store any confidential material or personnel info on any personal device or storage media (floppy disks, CDs, etc.).
- Understand that the use of personal devices for County business may subject those personal devices to public records disclosure.

SECTION 7. ELECTRONIC COMMUNICATIONS TOOLS

This Section covers electronic communications tools including network-based electronic mail, scheduling, browsing, and information management capabilities. The electronic communications tools are County resources provided to assist in the conduct of County business. Except as allowed under this Policy, the electronic communications tools may only be used for County business.

A. E-Mail

1. Usage. E-mail is provided as a tool for the conduct of County business. Guidelines on risks and

cautionary advice are appended to this Policy. Employees may not use personal email accounts to conduct County business.

The e-mail system is maintained as a messaging environment and is not intended as a Personal Information Management or Project Management repository. Users are cautioned against depending on the system for these purposes.

E-mail communications must not be used improperly. Examples of improper use include but are not limited to:

- a) personal gain, personal business, or political ventures;
- b) soliciting junk mail or subscribing to newsgroups unrelated to County business;
- c) the sending of offensive messages; and
- d) personal use except in compliance with this Policy.

"Offensive" for the purposes of this Policy is broadly defined as containing information or images that would be considered inappropriate in the County workplace or that would contribute to creating a hostile work environment. Examples include, but are not limited to, content which could make others feel uncomfortable because of their treatment of topics involving gender, race, disabilities, or sexual matters or any other protected classification.

2. Group or General Circulation. As the County email system is available for the conduct of County business and is not available for the distribution of personal messages or to provide an avenue of communication for individuals, the System's ability to send a message to a select group, or to all Users, should only be used on a limited basis by those persons authorized to distribute all employee messages. Individual users do not have this authority and may face discipline for inappropriately using access to the email groups. All broadcast e-mail messages should identify the source by department and name. Responses to broadcast messages should be directed to the source only and not the group as a whole unless the originating message requested group response. When determining whether a message should be broadcast on a department-wide or countywide basis, make sure that you know your audience. Avoid broadcasting messages to people with whom you do not ordinarily have direct contact. Each department is responsible for broadcast e-mails sent by employees of the department. Procedures regarding the approval of such e-mail will be left to the individual departments.

The prohibitions for individual e-mail communications apply to group e-mail communications. Any departmental questions regarding a group message should be addressed to IT.

3. Public Records and Retention. Users are responsible for knowing and complying with the County Public Records Policy, which includes rules for email communication.

All emails will be purged from the email system once they have been in the system for more than two years. This duration may change. Emails which must be retained for a longer period of time should be saved in another format. Users are not to purge or "empty" emails from their mail boxes prior to this system level purging.

4. Confidential Information. E-mail should not be used to transmit confidential information unless it is appropriately protected through encryption. Users should rely on the assumption that any e-mail sent is not secure.

B. Internet Use and Browsing Software

Access to the Internet is provided as a tool for the conduct of County business. Many resources are available through Internet connections to assist employees in performing their work in a more efficient and effective manner.

Use of the Internet is a privilege, not a right, that may be revoked at any time for unacceptable use which could affect the ability of a users to perform the duties of their job. The County retains the right to keep, retrieve and monitor logs of all access to Internet and online service with or without notice.

All Internet activity is logged and this log may be reviewed and monitored to determine if inappropriate use has taken place. Access to inappropriate or questionable Internet sites may be blocked. If a User has a legitimate County related need to access a blocked site, an appropriate request explaining the basis for the need should be made to IT and the User's supervisor in advance.

Inappropriate use, including inappropriate personal use, of the Internet may subject the user to discipline, up to and including dismissal.

If a User inadvertently attempts to access an inappropriate site, that User should notify his/her supervisor and IT as soon as possible. Notification by email is appropriate, including an identification of the site inadvertently accessed.

Any Department Head, in coordination with Human Resources, has the authority to deny, revoke, suspend or close the access for any User supervised by that Department Head, at any time based upon a determination of inappropriate use by that User. IT also has the authority to suspend or close access for any User at any time.

Restrictions may be placed on the use of the Internet or online services to protect the County and its resources.

C. Telephones and Voice Mail

Telephones and the voice mail system are provided as a tool in the conduct of County business. Telephone and voice mail use should be consistent with this Policy including utilizing appropriate passwords and maintaining the security of the voice mail system. This Policy does not cover cellular telephones (see Personnel Rules for cell phone policy).

D. Fax Machines

Fax machines are provided as a tool for the conduct of County business.

E. Prohibited Use

No User shall visit, view, send, receive, or download obscene, profane or inappropriate content on the Internet or via email/voice mail, including, but not limited to: pornographic materials, ethnic slurs, racial epithets or any other materials that might be construed as harassment, disparagement, libel or discrimination based on gender, race, sexual orientation, national origin, religion, or political beliefs, except as necessary in the course of a criminal or internal investigation. Departments whose users may engage in this behavior in the course of a criminal investigation shall adopt internal procedures for reporting and tracking such usage.

SECTION 8. ACCESS AND PRIVACY

Users of the System have no right of privacy for any electronic record or communication. The County may access, view or listen to any electronic record or communication in the System with or without notice to the User regardless of whether it is business related or personal. Many voice and data systems create and maintain detailed records of user utilization. These activity logs are accessible for consideration in disciplinary actions and can be subject to public information requests. Employees designated to access records may include, but are not limited to, a User's Department Head or designee, representatives from the Human Resources Department, County Counsel's Office or IT.

The County reserves the right to alter, modify, re-route or block the delivery of messages as appropriate. This includes but is not limited to:

- Rejecting, quarantining or removing the attachments and/or malicious code from messages that may pose a threat to County resources.
- Discarding attachments, such as music or video, considered to be of little business value and of significant resource cost.
- Rejecting or quarantining messages with suspicious content.
- Rejecting or quarantining messages containing offensive language.
- Rejecting or quarantining messages determined to be unsolicited commercial email (spam).
- Appending legal disclaimers to messages.

The use of a password does not give rise to any right of privacy to any User. Deleting records does not necessarily mean that a record, communication, or document has been eliminated from the System.

Users are prohibited from engaging in any unauthorized transmittal, copying, modification or removal of data on County systems. Nor should any User provide unauthorized access to County systems.

SECTION 9. PERSONAL USE OF THE SYSTEM

The County does not prohibit personal use of the System (*e.g.*, sending e-mail over the Internet, accessing sites on the Internet, typing a letter, or making a local telephone call) provided that the use is infrequent and brief and is otherwise consistent with this Policy. The County reserves the right to determine what constitutes reasonable use of the system. The County recognizes that employees occasionally have a need to talk to family members, schedule service technicians, confer with children's schools, and take care of a variety of other matters during "regular" working hours and that, in today's electronic environment, use of the System for these purposes may be more efficient. The County believes that personal use for these purposes during regular working hours is less disruptive, provided that the use is brief, infrequent, and in compliance with the following guidelines and understandings:

- There is no right of privacy for any electronic record or communication, whether personal or not, on the System.
- The use of the County phone system for personal long-distance phone calls is prohibited, unless

placed by using a personal calling card or by calling collect. Personal calls of any type must be infrequent and brief.

- Personal communications to group "Bulletin Boards" or "Chat Rooms" is prohibited.
- Users shall not use any component of the System for illegal activities, engaging in profit making ventures, or any business with which an employee may be personally associated (other than County business). An example of "personal business" for purposes of this Policy is on-line stock trading or subscribing to a financial newsletter for delivery via County e-mail.
- Users shall not access sites containing pornographic or offensive materials. The County retains the right to define "offensive" when needed.
- Users shall not access nor play games on the County system.
- Users shall not listen to radio or television stations or view web sites that use streaming audio or video unless directly related to their job function.
- Users shall not download software or any information which requires storage on County equipment, not related to assigned job responsibilities.
- Users shall not attempt to gain unauthorized access to protected resources.
- Users shall not download music, videos or any other copyrighted material for personal use. Downloads of such material for official business are allowed only if the appropriate permissions, licenses or other authorizations are obtained and the downloading is approved by an authorized supervisor. Users who use the system to violate copyright laws shall be personally liable for any fines, penalties or other costs.
- The System shall not be used for political activity.
- The System shall not be used in any way for non-profit or charitable activity not officially sponsored by the County and approved by the Board of County Commissioners.
- Personal use shall usually occur during formal breaks or meal periods.
- The County system shall not be used for personal financial gain.
- The County system shall not be used for personal use of social media.

Limited personal use of the System is not anticipated to increase any hardware or software costs to the County and should not result in any charges or costs to the County provided this Policy is followed. However, if personal use by a User results in an additional fee or charge to the County, the User shall reimburse the County for this additional cost, or the market rate of such charge, if a County discount applies. Printing a personal e-mail message or letter on a County printer are examples of actions, which result in an additional cost.

Personal fax use is discouraged, but is allowed for infrequent use. Employees must reimburse the County the charge as indicated in the County's Public Records Fee Schedule.

Users are required to limit personal use of the System and apply sound judgment to any personal use. Significant personal use is prohibited. Misuse or overuse may be the basis for disciplinary action.

Employees are specifically warned that, in addition to any potential violation of this Policy, routine use of the System in order to avoid a financial detriment (including purchase of a computer or subscription to an Internet access provider) may be considered an ethics violation and subject an individual to penalties provided under State law.

SECTION 10. INCIDENT RESPONSE PLAN

Accidental and malicious attacks against government computer systems are common. Any indication that such an attack is occurring or has occurred shall be reported to IT immediately. Any password or login suspicious behavior or any evidence of breach of security will be reported by the User to IT immediately. IT will report incident information to appropriate authorities when appropriate. Communication regarding information security events and weaknesses associated with information systems shall be communicated to IT and to Users in a manner allowing timely corrective action to be taken.

If the potential incident involves an exposure related to CJIS data, the connection to the CJIS data shall be severed until the incident has been cleared.

Users shall utilize the form attached at the end of this Policy when appropriate to report incident events.

SECTION 11. CONTENT

All records, messages, and communications should be appropriate to a governmental agency, professional, and courteous.

SECTION 12. VIOLATION OF POLICY

Violation of this Policy may constitute just cause for disciplinary action up to and including dismissal.

SECTION 13. EFFECTIVE DATE

This Policy shall be effective immediately.

Change History

Version #	Approval Date	Effective Date	Brief Description
1	7/1/95	7/1/95	Reviewed by BOCC and approved as part of the Personnel Rules
2	2/2011	2/2011	Update
3	4/2015	4/1/2015	Update

Risks & Cautionary Advice regarding Email

- Electronic messages are legally discoverable and permissible as evidence in a court of law.
- Messages sent electronically can be intercepted outside the County as well as inside.
- Electronic messages typically cannot be unconditionally and unequivocally deleted. The remote possibility of discovery always exists. Use caution and judgment in determining whether a message should be delivered electronically instead of in person.
- Electronic messages are frequently inadequate in conveying mood and context. Carefully consider how the recipient might interpret a message before composing or sending it.
- Even though the County utilizes anti-virus software, virus infected messages could enter the County's System. Viruses, worms and other malicious code can spread quickly if appropriate precautions are not taken.
- Be suspicious of messages sent by people not known by you.
- Do not open attachments unless they are anticipated by you.
- Do not forward chain letters. Simply delete them.
- Unsolicited commercial email (spam) is a nuisance and a potential security threat. Do not attempt to remove yourself from future delivery of a message that you determine is spam.
- “Remove me” links are often used by mass junk e-mailers to verify that you exist. Process spam as directed by IT.
- Know when it's appropriate to send e-mail messages. Don't e-mail personnel items, bad news, or angry messages. These topics should be handled via phone, or, better yet, face-to-face.
- Ask yourself, “Does this e-mail message have a business purpose and is it vital to our daily operations?”
- Use the appropriate distribution list. Ask yourself “Who should receive this e-mail message?” A “your car lights are on” message does not need to be sent to people outside the building.
- When sending a reply to an e-mail message, determine whether you need to “Reply” to the original sender only or “Reply to All” to the entire recipient group. Beware of “Reply to All”—you might accidentally share your message with the entire agency.
- Always include a brief yet descriptive subject line. Avoid subject lines such as “Hey”.
- Keep it short. One of the benefits of e-mail is the ability to communicate quickly and concisely.
- Make sure your message contains all the important details: who, what, when, where, why, and how. Nothing is more frustrating to your readers than receiving a follow-up “oops” message.
- Take the time to do it correctly the first time.
- Because e-mail lacks the cues of body language and tone that are present in verbal communication, be careful with sarcasm and humor so that you are not misinterpreted.
- In “e-mail speak,” using all capital letters is SHOUTING and is considered rude.
- Use white space—put a blank line between paragraphs and keep paragraphs short. A screen with a lot of text is hard to read.
- Bold, italic, color, and font size do not always show up on computers that have different configurations, so don't assume the receiver will see what you see. For emphasis, use *asterisks* to catch a readers' eye. Also, graphic or clip art backgrounds don't always show up on the recipient's computer, so don't make design a vital part of your message.
- Before hitting that Send button, check your e-mail message for proper spelling, grammar, and punctuation.

SECURITY INCIDENT RESPONSE FORM

REPORTING FORM

DATE OF REPORT:

DATE OF INCIDENT:

REPORTING PERSON:

PHONE/EXT/E-MAIL:

LOCATION(S) OF INCIDENT:

SYSTEM(S) AFFECTED:

METHOD OF DETECTION:

NATURE OF INCIDENT:

INCIDENT DESCRIPTION:

ACTIONS TAKEN/RESOLUTION:

PERSONS NOTIFIED: