



BEFORE THE BOARD OF COUNTY COMMISSIONERS
FOR THE COUNTY OF TILLAMOOK IN THE STATE OF OREGON

In the Matter of Revising the Tillamook)
County Employee Policy & Procedures)
Regarding Communications and)
Software Systems)

ORDER
#09- 084

FILED
Jan
OCT 07 2009
TASSI O'NEIL
COUNTY CLERK

This matter came on to be heard this 7th day of October, 2009 at a regular meeting of the Board of Commissioners, at the request of Michael Soots, Information Services Director of Tillamook County and Dave Dickman, Director, Human Resources.

Being fully apprized of the records and files therein, the Board of Commissioners finds as follows:

- 1. The Tillamook County Employee Policy & Procedures Manual needs to be revised to expand the section on Communications and Software Systems to include policies and procedures due to advances in technology.

NOW THEREFORE, IT IS HEREBY ORDERED THAT:

- 2. Pages 23 to 27, attached hereto as Exhibit A, be included in the Tillamook County Employee Policy & Procedures Manual to revise the current section on Communications and Software Systems on Pages 23 to 27.
- 3. This order is to become effective on October 12, 2009.

DATED this 7th day of October 2009.

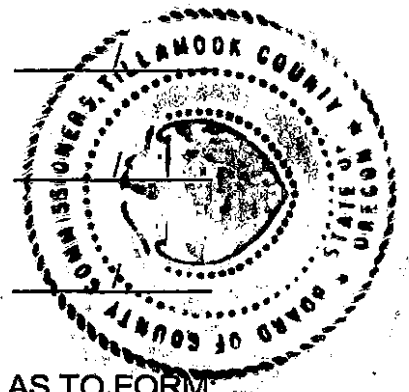
BOARD OF COUNTY COMMISSIONERS
FOR TILLAMOOK COUNTY, OREGON

Tim Josi
Tim Josi, Chairperson

Mark Labhart
Mark Labhart, Vice Chairperson

Charles J. Hurliman
Charles J. Hurliman, Commissioner

Aye Nay Abstain/Absent



ATTEST: Tassi O'Neil
County Clerk

APPROVED AS TO FORM

BY: *Dusan L. Becraft*
Special Deputy

William K. Sargent
William K. Sargent

EXHIBIT A

COMMUNICATIONS AND SOFTWARE SYSTEMS **Electronic Communications Systems**

The objective of this policy is to minimize the risks to business functions and government owned assets, and to assure adherence to regulatory and legal requirements.

All employees are required to attend yearly Information Services computer security training.

Tillamook County provides electronic communication systems to maintain superior communications both within the County and with outside parties. You are encouraged to learn about these tools and how to use them. This policy provides directions for you regarding access and disclosure of information when using these communication systems. All employees and others outside the County who may use the systems are expected to be aware of and support this policy. Department heads are permitted to issue their own policies that augment this policy, but not to supersede or contradict it. Departments that add an additional Policy in regards to Information Services Systems must inform the Information Services Department in writing and provide a copy of that policy upon completion.

Our electronic communications systems include computers, software, electronic mail (e-mail), copiers, fax machines, printers, telephones, voice mail, cell phones, pagers, and various on-line services. All of these systems are managed by the Information Services Department. Any software or other devices needed to perform your job needs to be requested in writing with business justification and reviewed for compatibility to the system by the Information Services Department prior to use.

No loading or downloading of software, freeware, Web Browsers, I-Tunes, Instant Messengers, or games of any kind may be done without prior written approval from the Information Services Director or their designee.

These systems and any other informational, storage, or retrieval services that the County provides are tools and are to be used for County purposes only.

The use of these systems is not private or confidential. Most communications are considered to be public record and subject to disclosure. Records that are exempt from public disclosure are defined in ORS 192.660. The County, within the bounds of current and future laws, reserves and intends to exercise the right to review, audit, intercept, access, and search these systems at will, monitor data and messages within them at any time for any reason, and disclose selected contents without notice or other restrictions. Messages sent through these systems remain the property of the County.

These systems shall not be used to receive unauthorized copyrighted materials, trade secrets, proprietary information, or similar materials from outside the County without prior authorization.

Any messages or communications used through this system are subject to our anti-harassment, anti-discrimination, and non-solicitation policies. You are expected to carefully compose and review the wording, tone, and content of your communications before transmission.

You should check with your supervisor if you have any questions about the proper use of communication or software systems. All system users who discover violations of this policy are expected to notify their supervisors or the Information Services Department immediately. Improper use or violation of this policy can result in disciplinary action, up to and including termination.

Passwords

The use of passwords for security does not guarantee confidentiality. You are to keep your individual passwords confidential and you should not access or attempt to access other employee's passwords. All passwords must be a minimum of 5 characters in length. Information Services recommends using strong passwords ie letter and number combinations.

ID Badges

Identification Badges are provided to all Tillamook County Employees and Volunteers. Badges must be worn at all times while on Tillamook County business. If your badge is lost or stolen report it to the Tillamook County Personnel office immediately.

Telephone Usage

The County realizes that employees must occasionally make and receive personal telephone calls at work. Such calls must be held to a minimum, and should impact your work as little as possible. Unauthorized or improper use of the telephone, including County provided cell phones, and charging long distance calls to the County, must be repaid, and misuse may result in corrective action, up to and including termination.

Voice Mail System

The voice mail system at the County belongs to the County and is provided for use in conducting County business. All communications and information transmitted by, received from, or stored in this system are County property. The voice mail system is to be used for County business only and use of the system for personal purposes is prohibited. You have no right of personal privacy in any matter stored in, created, received, or sent over the voice mail system. The County in its discretion reserves and may exercise the right to monitor, access, retrieve, and delete any matter stored in, created, received, or sent over the system, for any reason and without employee permission. You are not authorized to retrieve or listen to any voice mail messages that are not sent to you. Any exception to this policy must receive prior approval from management officials with authority to waive the policy.

Electronic Mail System

You are reminded to be courteous to other users of the e-mail system and always conduct yourself in a professional manner. E-mail messages are sometimes misdirected or forwarded and may be viewed by persons other than the intended recipient. You should write e-mail communications with no less care, judgment, and responsibility than you would use for letters or internal memoranda written on County letterhead. As with all other communications, email messages are part of the public record and may be subject to disclosure.

You should know that even when a message is erased through e-mail it is still possible to retrieve and read that message. We expect employees to respect others' privacy, and not retrieve or read electronic messages unintended for them unless authorized to do so. Using a

County e-mail address when posting to public forums (e.g. blogs, wikis, Twitter) and discussion lists for personal use is prohibited.

Tillamook County Computers, PDA's and Cell Phones

To protect the integrity of our systems only hardware supplied by the County can be connected to the system. An employee will not connect any personal hardware that is not purchased through or authorized by the Information Services (IS) Department. Use of County computer, peripherals, and networks for non County business is prohibited.

All software used on County equipment must be registered and approved by the Information Services Department and the software media and license on file in the Information Services department. Copy or transfer of County-owned software is prohibited. Personal or downloaded software for business purposes may only be installed after written authorization from the Information Services department. A virus check of all such software must be performed immediately before it is installed on any County equipment.

The use of personally owned technology for conducting County business, where official County records are created but not maintained by the County is prohibited.

USB / Flash Drives / Removable Storage Devices

All USB/Flash drive/Removable storage devices must be virus scanned before being used on any County computer system. All USB/Flash drive/Removable storage devices must be approved by the Information Services Department prior to use. All sensitive county data placed on removable storage devices drives must be encrypted and secured via approved encryption levels. Using encryption technology that has not been approved for use by the County is prohibited.

Sensitive data is considered to be:

- Any data (documents, spreadsheets, databases) that contains any Patient medical information. (HIPAA)[45 C.F.R. parts 160 and 164],[O.R.S 646A.622(c)]
- Any data that contains personal identifiable information [O.R.S 646A.602(11)] (names/SSN's/phone numbers/addresses/anything that can be used to facilitate identity theft (e.g., mother's maiden name).
- Any financial information (bank account numbers, tax information, credit card information)
- Any other data required to be protected by the county

A virus check must also be made of any portable media (anything that holds data and can be transported) originating or used on any computer outside of the County system prior to use on a County computer.

Credit Card / Check Processing

Tillamook County processes credit card transactions and checks through devices attached to computers on the Tillamook County network. Data security is a major concern for the County. Any computer used for credit card/check processing shall be classified as high security equipment. Internet usage is strongly discouraged and may be prohibited on these machines. Personal internet usage on these machines is prohibited. Computers used for payment processing will be monitored for internet usage. Employees using these machines or

processing credit card/check payments are required to attend additional security and cash handling training on a yearly basis.

Internet, Messaging, Other Usage

County policies regarding acceptable behavior and communication will apply to the use of the Internet and messaging. Specifically prohibited use includes but is not limited to:

Internet:

- Use of social networking sites for personal use;
- The use of unauthorized "Soft" VOIP(Voice Over Internet Protocol) phones, e.g. Skype, Vonage, etc.;
- The use/installation of unauthorized Instant Messaging, e.g. AIM, Yahoo Instant Messenger, Meebo, IRC, etc.;
- Links and attachments are prohibited using the authorized IM client;
- No Peer to Peer Networking, e.g. E-Mule, Kazaa, Limewire, Warez, etc;
- Using security exploit tools (hacking tools) to attempt to elevate user privileges or obtain unauthorized resources;
- Accessing sites that distribute computer security exploits ("hacking" sites);
- Accessing inappropriate sites including adult content, online gambling, and dating services;
- Accessing sites that promote illegal activity, copyright violation;
- Excessive use of online shopping;
- Use of streaming media (Audio/Video) for entertainment during work hours;
- Using the internet to obtain or disseminate language or material which would normally be prohibited in the workplace;

Email:

- Making unauthorized general message distributions to all users (everyone);
- Broadcasting e-mail to large numbers of constituents unless the list members are hidden through the use of the BCC field.

Other:

- Conducting a private business;
- Political campaigning;
- Installing any software that has not been approved by the County Information Services Department;
- Sharing or storing unlicensed software or audio/video files

If any of the above prohibited uses is required for a legitimate business reason, it is management's responsibility to follow the exception process below.

EXCEPTION PROCESS

Exceptions to this policy must be requested by management via an Information Services Request form. Exceptions will be documented in writing and retained according to existing retention schedules. Exceptions may be granted on a limited-time basis.

POLICY ENFORCEMENT:

In order to safeguard County resources, violators of this policy may be denied access to County computing and network resources and may be subject to other disciplinary action within and outside the County. Violations of this policy will be handled in accordance with the County's established disciplinary procedures. The County may temporarily suspend, block or restrict access to computing resources and accounts, independent of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, confidentiality, or availability of County computing and network resources, or to protect the County from liability.

If violations of this policy are discovered, the County will take appropriate actions to resolve the issue and violators may be subject to disciplinary measures up to and including termination

If violations of this policy are discovered that are illegal activities, the County will notify appropriate authorities.

The County reserves the right to pursue appropriate legal actions to recover any financial losses suffered as a result of violations of this policy.

Employee _____

Date _____

Manager _____

Date _____