Computers, Technology & Information Security

Revision: 2
Date: 10/28/13
Original Issue Date: 11/17/11
Number of Pages: 2
Approved: BOCC

Teton County email, computer, internet, copier, phone and voice mail systems are County property provided to further County business. Employees are expected to use these various information technologies in a responsible manner and to use good judgment to protect the physical and electronic integrity of all equipment, networks, software and information.

Employees should have no expectation of privacy when utilizing any of the County's information systems. The County reserves the right to intercept, monitor, copy, review and download any communication or files created or maintained on the County's Information Technology (IT) systems. Incidental personal use is allowed provided it does not interfere with work, consume County resources or create potential County liabilities.

Teton County maintains two separate computer networks: one for the Sheriff's departments and another for all other departments. The County may hire an employee, or contract with outside firm(s), to administer and maintain the county's computer network(s), equipment and software. At least annually, the Board of County Commissioners will designate who is currently serving as IT Administrator.

Purchase & Installation of Computer Equipment and Software. Teton County maintains a standard configuration for all networks and systems. Purchase and proper installation of network-compatible hardware and software is critical for the proper operation of the county's networks and efficient use of county dollars. In order to maintain network integrity, written approval must be received from the IT Administrator *before* the purchase of any computer, software, printer, scanner or other peripherals*.

In general, computers should be replaced every four years.

The County's IT staff and contractors are the only personnel authorized to add or remove computer hardware, software or peripherals from computers connected to the County networks. Employees who perform unauthorized work on the county networks may be subject to disciplinary action.

**Peripherals include laptop computers, wireless access points, mp3 players, digital recording devices, etc.*

Disposal of Computers and other IT Equipment. Any personal property no longer necessary for county use must be disposed of by the Board according to Idaho Code 31-808, or 31-829 if the Board determines the asset has greatest value as a trade-in. Idaho law allows personal property valued at $250 or less to be sold at private sale without notice. The IT Administrator shall take custody of all surplus computer equipment in order to remove all county-specific data and software and determine its estimated value. Equipment valued more than $250 must be sold at a public auction. A notice of such auction must be published at least 10 days prior to the date of auction. Equipment valued less than $250 may be sold to employees via a county-wide lottery or auction. Failure to dispose of personal property as described above may result in criminal penalties. *No computer may be disposed of until all county-specific information is permanently deleted from the hard drive.*

Software. Teton County purchases and licenses the use of various computer software programs for business purposes and does not own the copyright to this software. Unless authorized by the software developer, Teton County does not have the right to reproduce such software for use on more than one computer. Employees may only use software on local area networks or on multiple computers according to the software license agreement. Illegal duplication of software and its related documentation for personal use is prohibited.

Internet. Employees must remember that internet access is provided to enhance County functions. Incidental personal use is allowed only as described above. Downloading of copyrighted, protected materials or software is strictly prohibited. Streaming videos and/or music is prohibited unless necessary to complete a required task. (This activity diminishes internet response time county-wide and allows viruses to enter the system.) Prohibited internet sites include, but are not limited to, those containing offensive graphics, images and language. The County reserves the right to monitor all internet activity.

Social Networking. Use of social networking sites during work hours is not allowed unless required for a specific work task. Employees using social networking sites during personal time away from work are encouraged to remember that all postings become a matter of public record and may become part of the

employee's personnel file. Employees should also refer to the County's Personnel Policy, Chapter III.C which prohibits employees from engaging in behavior designed to create discord and lack of harmony among County employees and/or departments. Supervisors are discouraged from "friending" employees on social media sites.

Email. Email and internet access is provided by Teton County to enhance communications and provide access to work related information and technology. *All employees must remember that email is "Evidence Mail" and is subject to public records requests.* Employees should always ensure that the business information contained in email messages and other transmissions is legal, accurate, appropriate and ethical. Employees should not open email from unknown senders or that seems suspicious. Employees should follow established procedures for protecting files, including managing passwords and storing backup copies of files.

The following are examples of *prohibited uses* of email and internet systems:

- Sending or posting discriminatory, harassing, or threatening messages or images
- Using Teton County time and resources for personal gain.
- Sending or posting messages or material that could damage Teton County's reputation.
- Participating in the viewing or exchange of pornography or obscene materials.
- Using streaming audio, video or real time applications such as stock ticker, weather, or internet radio.
- Sending or posting messages that defame or slander other individuals.
- Attempting to break into the computer system of another organization or person.
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities.
- Using the internet for political or religious activities, or any sort of gambling.
- Passing off personal views as representing those of Teton County.
- Sending anonymous email messages.
- Unauthorized participation in or use of chat rooms or instant messaging.
- Logging on or using another employee's computer without authorization.
- Engaging in any illegal activities.

Telecommuting / Remote Access. Telecommuting (working from home or elsewhere) requires the specific, written pre-approval of a department head or elected official. Such written approval must be obtained before an employee begins working off-site and a copy must be given to the Human Resource Clerk. Employees may not remove any original files or documents from the worksite.

Access Codes & Passwords. The confidentiality and integrity of data stored on county computer systems must be protected by access controls to ensure that only authorized employees have access. Stealing, using or disclosing someone else's code or password without authorization is prohibited. Attempting to access restricted files or portions of operating systems or administrative systems is prohibited.

Information Security. Credit card numbers, log in passwords, social security numbers and other parameters that can be used to gain access to goods or services must not be sent over the Internet or via email. When documents containing such numbers and passwords are disposed of, they should be shredded and not thrown into the trash.

Credit Cards. Offices which accept credit cards should not create a written record of someone's credit card number unless absolutely necessary. If a written record is created, the document must be shredded immediately after the transaction is completed. Credit card processing devices must be secured at all times.

New Employees. At least 5 working days prior to a new employee's first day of work, the responsible supervisor must provide the following information to the IT staff: the new employee's name and job title, who they will report to, and what computer equipment they will be using.

Terminating & Transfering Employees. The responsible supervisor must notify IT staff immediately of any terminations or transfers involving a change in employee status. Involuntary terminations must be reported concurrent with the termination. Upon termination, the county will deny all access to county software and e-mail. The responsible supervisor will be responsible for obtaining any digital devices issued to the terminated employee.