Marion County OREGON

ADMINISTRATIVE POLICY

SECTION:	**Information Technology**			**POLICY #:**	**701**
TITLE:	**Use of Computing and Communications Assets**			**PROCEDURE #:**	
				ORDER #:	**16-87**
DEPT:	**Information Technology**			**DIVISION:**	**IT**
ADOPTED:	**12/92**	**REVIEWED:**	**10/94, 1/04**	**REVISED:**	**7/16**

PURPOSE:

County computing and communications assets consist of hardware, software components, data, and internet-based services. Proper use of these assets is necessary to provide reliable, accessible, and relevant services and to protect the data needed to support these services.

Hardware includes telephones, computers, servers, routers, multi-function copiers, mobile data systems, modems, scanners, and other office equipment which can be used to send, receive, manipulate, or store county data. This would also include peripheral devices such as thumb drives, external hard drives, tapes, etc.

Software includes programs, tools, utilities, and metadata used to store and access information related to county services and operations. Software may be implemented on county owned equipment or hosted by entities with which the county has entered into contractual relationships. Software includes but is not limited to:

- Business program specific applications
- Enterprise-wide applications such as operating systems, electronic mail (email) and browsers
- Mobile device applications
- Reporting tools
- Network and database administration tools

Services include dynamic and contracted delivery of intangible functionality such as Internet access, storage, instant messaging (IM), and phone connectivity. Services are used by county employees and volunteers to carry out their assigned responsibilities efficiently by expediting communication within the county, with other agencies, and with the public.

This policy is being established to authorize Marion County Information Technology (IT) to develop, implement, utilize, enforce, and evolve the processes and procedures needed to ensure appropriate use of computing and communications assets.

SUBJECT: Use of Computing and Communications Policy

AUTHORITY: The Marion County Board of Commissioners may establish rules and regulations in reference to managing the interest and business of the county under ORS 203.010, 203.035 and 203.111.

The Marion County Board of Commissioners expresses the governing body's formal, organizational position of fundamental issues or specific repetitive situations through formally adopted, written policy statements. The policy statements serve as guides to decision making for both elected and appointed officials on the conduct of county business.

The Marion County Administrative Policies and Procedures manual of the Marion County Board of Commissioners outlines the forms and process through which the board takes official action on administrative policy, and is the official record of county administrative policy.

APPLICABILITY: All county departments, employees, contractors, business partners, and volunteers.

GENERAL POLICY: Marion County has an overriding interest and expectation in deciding how to best utilize computing and communication assets. This policy establishes guidelines for use and management of these assets.

POLICY:

1. Responsibilities:

1.1 Computing and communications assets (hardware, software, data, and services) acquired by the county are to be used for official county business functions.

1.2 The provisions of this policy apply for all use of county computing and communications assets through direct connection to the county network, connection via county wireless network, and through remote access (see Administrative Policy 705: Remote Access).

1.3 All computing and communications assets, including data, are property of Marion County. All computing and communications assets used for the electronic creation, translation, and manipulation of data in any form are subject to inspection by the county, as are the resulting data stores.

1.4 Incidental, personal use of these assets is permitted consistent with this policy and department guidelines and is subject to the standards of the Oregon Government Ethics Commission. Examples of acceptable incidental use include talking with family members on matters requiring attention during normal business hours, making medical and service technician appointments, and talking with a child's teachers or school administrators.

1.5 Incidental use is a fringe benefit (i.e., as part of "official salary") under ORS 244.040 (1) (a). The value of this benefit is incidental, and the county will not impute income to the employee's salary for the value of the fringe benefit. If the appropriate taxing authority

determines that an employee's use of county equipment, hardware, software, and services constitutes "income" to the employee, then the employee and not the county shall be responsible for payment of taxes.

1.6 There is no expectation of privacy as to any data, including files, voicemail, images and/or text messages, that is transmitted, stored or received on county computing or communications assets provided or paid for by the county.

1.7 Employees shall not use county computing and communications assets for private business activities.

1.8 Any message or wording that degrades or humiliates any person is strictly prohibited. Comments made, copied, stored, forwarded, or otherwise transmitted on any county computing or communication device shall adhere to approved Human Resources (HR) policies and guidelines (See Policies 602 and 603).

1.9 Forwarding, copying, or distributing confidential or restricted material using county computing and communications assets without proper authorization is prohibited.

1.10 IT Director or designee approval is required for purchase, lease, or subscription use of any computing and communication asset.

1.11 No one other than Information Technology Department staff, or service providers working within the provisions of an executed contract or service agreement, shall install, move, remove, or alter county computing and communications assets.

1.12 Employees shall log off or lock assigned computing or communications assets when taking breaks, leaving work, or when said device will be left unattended by the assigned employee. In no case should any computing or communications assets be left unsecured or unattended when confidential or restricted information is displayed on the screen.

1.13 Personal use of electronic distribution groups is not allowed.

1.14 Software and Hardware

- 1.14.1 County owned, licensed, or subscribed computer software shall not be copied for personal use.
- 1.14.2 To minimize risk from data-destroying viruses, only software, hardware, services, and storage media owned, licensed, or subscribed by Marion County shall be used to store, access, or manipulate county data. Exceptions such as trial installations to ensure business needs are met prior to purchase may be approved on an individual basis by the Information Technology Director or designee.
- 1.14.3 Copying computer software, data, text, graphic, audio-visual, or "multi-media" material may violate copyrights and may constitute a crime under federal law. Copyrighted software shall only be copied by the IT Department for backup, archive, or deployment purposes and only in accordance with contractual, licensing, or subscription agreements. Duplications of copyrighted software or documentation for any other purpose is prohibited.

1.14.4 Public domain or shareware software shall not be used on county-owned computing and communications assets. Exceptions may be approved on an individual basis by the IT Director.

1.15 Email

1.15.1 Email-related policy applies to electronic mail accessed through any county computing or communication asset.

1.15.2 All communications, texts, metadata, images, files, and attachments created, stored, or distributed via email are considered public records, available for public inspection unless specifically exempted by state law.

1.15.3 Email messages and attachments shall be retained in accordance with Oregon Administrative Rules (OARs) and county retention policy.

1.15.4 All email communications are subject to inspection at any time without notice by the county.

1.15.5 Mass distribution groups may only be used for official county business. Use of certain mass distribution groups (such as AllCounty) must be authorized by a department head or elected official or designee. Responses to mass distribution emails shall be directed to the sender and/or specifically relevant parties only.

1.16 Instant Messaging

1.16.1 Instant messaging applies to text-based communication sent or received on any county computing or communication asset or on personal devices when the content relates to county business.

1.16.2 All communications distributed via instant messaging are considered public records, available for public inspection unless specifically exempted by state law.

1.16.3 Instant messaging shall not be used for matters dealing with disciplinary or personnel performance issues.

1.16.4 Instant messages will be logged and retained in accordance with Oregon Administrative Rules (OARs) and county retention policy. The default retention period for instant messages is 90 days.

1.16.5 All instant message communications are subject to inspection at any time without notice.

1.16.6 Use of group messaging (group chat) may be used only for official county business and should include only those parties directly related to the specific business topic.

1.17 Internet

1.17.1 Internet access is provided as a resource and tool for assisting in the execution of official county business.

1.17.2 Due to the high risk of viruses, no executables or program files may be downloaded to county computing or communications assets except by IT Department staff. Exceptions may be approved on an individual basis by the IT business manager.

1.17.3 Downloading copyright protected files, programs, images, text, or other information resources is allowed only in accordance with contractual, licensing,

or subscription agreements. The person downloading material is responsible for ensuring that no copyright protection will be violated.

1.17.4 Elected officials and department heads may establish more restrictive Internet use policies for their departments.

1.17.5 An elected official or department head may, with approval from HR or the Legal Department, request the IT Department to implement software to limit, restrict, and/or monitor employee Internet access at any time and without notice.

1.17.6 Use of internet email is subject to the standards outlined in Section 1.15 of this policy.

1.17.7 Employees may not post, distribute, store for retrieval, or otherwise make accessible via the internet any of the following:

- Defamatory, derogatory, insulting, or degrading material or information
- Confidential, restricted, or privileged information
- Copyrighted materials without the express consent of the copyright holder

1.17.8 Employees may not use anonymous Internet identities to conduct county business nor while using county computing or communications assets.

1.17.9 Transmission of confidential or restricted information via the Internet/Intranet requires authorization by the department head or elected official in conjunction with the IT business manager. Confidential or restricted information approved for such transmission must be encrypted.

1.17.10 The county budget may provide funds for computer subscription services such as online training or storage services. Such services must be reviewed and approved by the IT Director prior to purchase. Supervisors are responsible for monitoring proper use of these subscription services.

1.17.11 Access to sites containing racist, violent, or sexual content is strictly prohibited except as required for execution of assigned tasks and authorized by the department head or elected official.

1.18 Mobile Data Systems

1.18.1 Mobile data systems combine components of email and online computer subscription services. The policies applicable to email and online subscription services apply to these systems.

1.19 Passwords

1.19.1 Employees are required to select and maintain individual passwords for access to the county's computer network.

1.19.2 Employees must disclose their passwords to their supervisor or manager upon request for any system having passwords which cannot be reset by IT to provide access to department business records not available by other means. Upon completion of the action requiring disclosure, the employee is required to establish a new password for ongoing use.

1.19.3 Employees shall store documents in directories accessible only to the appropriate business users.

1.19.4 Other than as noted in 1.19.5, employees shall not use another employee's password to gain access to that employee's files or the computer network.

1.19.5 Each department head or elected official may provide passwords to employees authorized to serve as designees to ensure access to data needed for continuity of business operations.

1.19.6 HR, Sheriff's Office or Legal may authorize bypassing or changing a user's password or accessing a user's email or other files otherwise accessible only with that user's password as required to conduct investigations for their respective roles.

1.19.7 When users are provided passwords to access external services, private or governmental, they shall not divulge the passwords to anyone in violation of the terms and conditions of the service that issued or required the password. Any disclosure of these passwords will only occur upon specific authorization of a user's supervisor or manager.

1.20 Encryption

1.20.1 Employees shall not encrypt files or email communications without advanced approval from their department head or elected official.

1.20.2 For approved uses of encryption, employees will work with IT to identify the appropriate encryption tool(s) to be used.

1.21 Access to Computer Files

1.21.1 Departments must notify IT in a timely manner when an employee or volunteer leaves county service. It is the responsibility of IT to obtain and change all relevant passwords and execute the proper disposition of any saved data based on county retention guidelines.

1.21.2 The HR and/or Legal Department may authorize access and retrieval of an employee's or other county user's voice mail, email, instant messages, computer files, and related data. This access may occur without notice and without cause.

1.22 Telephones

1.22.1 Employees shall not make personal long-distance telephone calls on land-line county phones. For information and policy on the use of cellular telephones reference Administrative Policy B20.

2. Exceptions:

Exceptions may be granted only as noted above.

3. Implementation:

The IT Director is authorized to implement and execute this policy.

4. Violations:

The proper use of county computing and communications assets enhances productivity and allows the county to meet increased service needs. It is the responsibility of each county employee to use these assets properly. It is the responsibility of each county official and department head to ensure this policy is enforced.

Violation of the policies or procedures set forth in this policy may result in removal of unauthorized computing or communication assets. Violations may also be grounds for disciplinary action up to and including termination of county employment.

5. Periodic Review:

This policy will be reviewed by the IT Director and County Legal Counsel every two years and updated as needed.

Adopted: 12/92

Revised: 10/94, 1/04, 7/16