XXX.XX – Authorized Use of County Resources, Including Information Technology Systems
Stakeholder Review: 9/14/21-10/14/21

Refer:
- ORS Chapter 244, Government Ethics
- Multnomah County Personnel Rule 3-30, Code of Ethics
- Multnomah County Personnel Rule 3-35, Use of Information Technology
- Multnomah County Personnel Rule 3-36, Social Media
- Multnomah County Personnel Rule 3-37, Cellular Devices
- Multnomah County Personnel Rule 4-20, Benefits
- MCSO Policy 400.00 – Code of Ethics
- MCSO Policy 1205.00 – Use of Social Media
- MCSO Policy 1200.00 – Communication with the Media

Definitions:
- Information Technology Systems – Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

Policy:
1. The Multnomah County Sheriff's Office encourages the use of County resources and information technology systems to support the mission and business of the County. The appropriate use of all County resources is the responsibility of each member and relates directly to official activity which the member was hired to perform. Resources shall be used for their intended purpose in accordance with the law (e.g., state, local, contracts, licenses, property rights, records, etc.), policy, procedure, or training.

2. Members are entrusted with the use of County resources such as facilities, office fixtures, office supplies or equipment, electronic and physical records, uniforms and equipment, information technology systems, and vehicles. Less obvious examples of County resources include work time, data, and information. During non-work times, members are permitted brief and infrequent personal use of county systems if the use does not interfere with official business, is at virtually no cost to the county and is in accordance with state ethics laws and rules. Unauthorized or inappropriate uses of resources include, but are not limited to, facilitating unauthorized access or modification, negligent or purposeful misuse, abuse, breach, damage, destruction, loss, or theft. Members who use County resources in such fashion will be subject to corrective action.

3. All information technology systems created or stored on County-owned systems are considered County property. Access procedures, such as the use of passwords, are meant to protect the security of County information technology systems and data. Members shall have no expectation of personal privacy or exclusion from monitoring in the use of County-owned systems.

4. The County may trace, review, audit, access, intercept, block, restrict, screen, delete, recover, restore, publish, or disclose any information on County-owned systems at any time without notice unless prohibited by law. The County has the right to access, monitor and record all electronic and voicemail or other County-owned systems at any time and without notice unless prohibited by law. Work records located on personal devices used for work purposes may be subject to Oregon's Public Records Law and other applicable laws and policies. Members are required to preserve work records contained on personal devices, and are required to produce such records upon request.

5. The use of County resources could invoke a collective bargaining provision(s) or right(s). In the event there is a conflict between a County right and a collective bargaining provision or right, the collective bargaining provision or right prevails.

6. While members are issued information technology systems because they have a need to remain in contact with the public, other members, and the chain of command to conduct official business, the use of County resources generates public records and is subject to public records law (e.g., retention, confidentiality, disclosure).

Procedure:

1. Member Responsibilities:
   1.1. Members are required to appropriately use County resources; when posting on the internet for non-work purposes, members may not use their county job title, contact information, uniform, or other information showing county affiliation in a way that indicates they are acting as County members.

   1.2. Members shall protect County information technology, including computer and mobile devices, and shall not share access to accounts, privileges, and associated passwords, unless there is a legitimate workplace need. Members shall not reveal their login credentials without supervisor approval.

   1.3. Members are prohibited from forwarding information related to Criminal Justice Information (CJI) (e.g., emails, calls, texts, images, data, recordings) to a personal smart phone or computer device. Members who do forward CJI violate Criminal Justice Information System (CJIS) regulations and may be subject to corrective action.

   1.4. Members are required to report inappropriate uses to their supervisor or up the chain of command.

2. Command Responsibilities:
   2.1. Command members shall:
      2.1.1. Educate their direct reports on proper use of County resources (e.g., standard operating procedure, direction or demonstration, coordination of training, etc.).
      2.1.2. Ensure County resources are managed (e.g., acquired, assigned, used, inspected, modified, repaired, replaced, etc.) in proper order.
      2.1.3. Investigate reports of inappropriate use by members and refer allegations of misuse to the Professional Standards Unit, if necessary.

   2.2. Agency or County-wide communications (e.g. email, flyers, etc.) require Agency authorization. Events which mix county and personal business, such as charitable drives, celebrations, or whatever the Agency deems suitable related to Agency business may be published with Chief Deputy authorization.

History:

- *Originating Policy and Procedure:*
- *Next Review Date:*
- *Review By: Sheriff's Office*

Please provide feedback here: https://forms.office.com/g/acmRpkqFxv