ADMINISTRATIVE POLICY

SECTION: 600 – Information Technology	**POLICY#:** 602
TITLE: Information Technology User Policy	**R & O #:** 17-28
	IMPLEMENTED BY PROCEDURE #: N/A
SPONSORING DEPT/DIV: Department of Information Technology Services (ITS)	
ADOPTED: 02/28/2017	**REVIEWED:** 11/28/2023

PURPOSE: The purpose of this policy is to:

1. Establish acceptable practices for use of information technology in the conduct of County business.
2. Establish that the County has a right to access any information technology that it owns and/or controls.
3. Ensure awareness that the use of information technology in the conduct of County business is subject to Oregon Government Standards and Practices Laws. In general, these laws prohibit any workforce member from using their official position as representatives of the County to obtain financial benefit or avoid financial detriment.
4. Ensure that the County maintains and stores all electronic information and communications created, processed, or stored in the conduct of County business in compliance with Oregon Public Records Laws and civil litigation.
5. Protect the County against damaging legal issues and cyber related security threats.

APPLICABILITY: This policy applies to:

1. All workforce members engaged by the County to use information technology in support of County business. This includes but is not limited to employees, contractors, consultants, temporaries, volunteers, and interns.
2. All information technology owned and controlled by the County as defined below.

DEFINITIONS:

Workforce Member: All authorized personnel engaged by the County to use information technology in support of County business. This includes but is not limited to employees, contractors, consultants, temporaries, volunteers, and interns.

Stipend Program: Allows qualifying employee's reasonable compensation for the use of a personal cell phone or Smart Phone for County business. Personal use limitations are removed from mobile communications devices subsidized under the stipend program, but ITS User Responsibility Policy guidelines continue to apply to the extent the device is used to access the Technology Environment.

County Owned and Controlled Technology: The County owns and controls the following information technology. This includes but is not limited to:

1. All electronic networks (including internet connectivity), devices and portable mass media either purchased, leased, administered, contracted through a third-party vendor, or otherwise under the custody and control of the County.
2. All electronic information and communications created, processed, or stored on networks and devices owned and controlled by the County.
3. All electronic information and communications relating to County business regardless of where the records are stored, including but not limited to, on personally owned devices, portable mass storage media, the "cloud" or externally provided services and personal email services.

Electronic information: Includes communications or data generated, processed, and/or stored for County business purposes, or that impacts the County in any way regardless of the physical location of the data (including personally owned devices and Internet) or the means through which data is accessed are County property. Also includes but is not limited to word processing documents, spreadsheets, graphs, charts, presentations, databases, calendars, telephone records and voice mail, internet data, logs, archives, backup or disaster recovery systems, and electronic communications (includes electronic infrastructures and networks, network-based electronic mail, scheduling, browsing, phones, voicemail, and information management capabilities). All County Electronically Stored Information (ESI) is considered an electronic public record subject to Oregon Public Records Laws.

Electronic Infrastructures and Networks (Voice and Data): Enterprise Data Network (physical, wireless, voice and VPN networks) including but not limited to:

1. All infrastructures, systems services, and interfaces.
2. Associated data and voice network, their components, systems, and email accounts.
3. Tape backup systems.
4. Landline phones, voicemail.
5. All owned or leased computing and telecommunication systems, programs, software, applications (including internet applications purchased by the County), databases, services, resources, or capabilities.
6. All environments for processing and storing any form of County ESI whether physical or virtual, within the County enterprise network or hosted on resources outside the agency.

All systems presenting content related to the County or facilitating any type of electronic communication or web-based interaction related to County business. County assets include but are not limited to the following:

1. Connectivity services: Includes but are not limited to:
    a. Outlook Web Access (OWA) allows all workforce members with assigned email accounts access to County email and calendaring remotely through any browser-equipped Internet connection. If you require assistance on how to use OWA or require remote access to your basic County email and calendar services beyond what you can access from your personal computer, contact the ITS Helpdesk.
    b. Virtual Private Network (VPN) and remote-control solutions (such as LogMeIn, WebEx, etc.) extend full capabilities to workforce members from outside the physical boundaries of the County enterprise network. Remote and VPN access to the County's physical network/infrastructure/data is attained through sponsorship from your supervisor. Contact the ITS Helpdesk for more detailed information regarding Washington County ITS Remote Work & Telecommuting Solutions.
    c. Mobile Data Management (MDM) - Only mobile devices provisioned through County ITS are capable of synchronizing with County email and calendaring. ITS identifies three classes of County participants as MDM users: users of County-owned devices, stipend-based workforce members who utilize personal devices and workforce members who utilize their personal devices without the stipend.
2. Electronic Devices: Includes, but are not limited to:
    a. County workstations physically connected to the County's network.
    b. Mobile Communications/Computing Devices - Includes but are not limited to notebooks, laptops, personal digital assistants (PDAs), tablets, cellular phones, Smart Phones (a smart phone is a mobile phone that includes advanced functionality beyond making phone calls and sending text messages. Most smart phones have the capability to display photos, play videos, check, and send e-mail, and surf the Web. Modern smart phones, such as the iPhone and Android based phones can run third-party applications, which provides limitless functionality), handheld wireless devices, and any other existing or future mobile computing or storage device.
    c. Portable Mass Storage Media: Include but not limited to plug-ins, Universal Serial Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives and any other existing or future portable mass storage media.

GENERAL POLICY:

It is the policy of the County that information technology is a county resource and tool to assist in the efficient conduct of County business. This technology is composed of electronic infrastructures and networks (data and voice), use of the Internet, electronic devices, and portable mass storage media and electronic information (including electronic communications). Unless otherwise specified by initial agreement, use of the County's owned and controlled information technology shall be conducted in accordance with this policy.

Use of information technology to conduct County business, is neither personal nor private. With a warrant or court order, the County has legal right to access any County owned and controlled information technology that stores electronic information at any time without knowledge or consent of a workforce member.

This policy requires all workforce members to read and understand this policy and to certify their completion of the County's Security Awareness Training (SAT) every year. All new Washington County workforce members must complete of the SAT within 30 business days of their first day of work.

POLICY GUIDELINES:

1. Responsibilities:
   In accordance with this policy, workforce members will exercise good judgment regarding appropriate and personal use of the County's information technology.

   Information Technology Services is responsible for administering and completion tracking for County Security Awareness Training.

   - All new County workforce members must undergo County Security Awareness Training within 30 days of their first day of work.

   - All County workforce members are required to recertify annually within 30 days of the County's Security Awareness Training (SAT) enrollment notification. Recertification requires all workforce members to read and understand this policy.

   Department Directors and Managers are responsible for enforcing compliance with this policy by ensuring that their workforce members complete all assigned security awareness training modules. Non-compliance can lead to disciplinary action as defined in the Washington County Personnel Rules and Regulations Policy.

   County workforce members who do not have a County email address but have access to the County network must provide proof to their County Department hiring authority that they have completed a Security Awareness Training provided by a certified external provider.

2. Exceptions:
   Exceptions may only be granted by the Washington County Board of Commissioners unless such authority has been delegated to the County Administrator.

   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.

3. Implementation:
   This policy replaces the former Information Technology User Policy approved on February 28, 2017, and previously revised on March 28, 1998, November 13, 2002, and June 22, 2005.

   Elected officials and department directors are expected to be knowledgeable of, and shall be responsible for, implementing this policy within their respective departments. Observance of this policy is mandatory for all County employees and violation may result in disciplinary action, up to and including termination.

4. Periodic Review:
   This policy shall be reviewed by Information Technology Services every year.