Tillamook County, Oregon
10/29/2021 8:30:00 AM
Commissioners' Journal
CJ2021-00313

BEFORE THE BOARD OF COUNTY COMMISSIONERS

FOR TILLAMOOK COUNTY, OREGON

In the Matter of Adopting the Tillamook County Information Services Administrative Policies	))))	ORDER #21-057

This matter came before the Tillamook County Board of Commissioners on October 27, 2021, at the request of Damian Laviolette, Director, Information Services (IS). The Board of Commissioners, being fully apprised of the representations of the above-named person, and policies and files herein, finds as follows:

1. Tillamook County workforce members must be compliant with appropriate county administrative policy.

2. Tillamook County has created five new administrative IS policies, attached herein, regarding the best practices and procedures for the management and oversight of Tillamook County information systems and technologies.

NOW, THEREFORE, IT IS HEREBY ORDERED THAT:

3. The policies attached herein regarding the best practices and procedures for the management and oversight of Tillamook County information systems and technologies are hereby enacted.

//

//

//

//

//

//

//

//

//

Dated this 27th day of October, 2021.

THE BOARD OF COMMISSIONERS
FOR TILLAMOOK COUNTY, OREGON

	Aye	Nay	Abstain/Absent
Mary Faith Bell, Chair	Y		
David Yamamoto, Vice-Chair			✓
Erin D. Skaar, Commissioner	✓		

ATTEST: Tassi O'Neil
County Clerk

By: _____
Special Deputy

APPROVED AS TO FORM:

_____
Joel. W Stevens, County Counsel

ADMINISTRATIVE POLICY

SECTION: Information Services		POLICY: IS-1
TITLE: Use of Computing and Communications Assets		ORDER #: 21-057
DEPT: Information Services		
ADOPTED: 10/27/2021	REVIEWED: TBD	REVISED: TBD

1. **PURPOSE/OBJECTIVE:**

1.1 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.

1.2 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.

1.3 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:

1.3.1 Business program specific applications

1.3.2 Enterprise-wide applications such as operating systems, electronic mail (email) and browsers

1.3.3 Mobile device applications

1.3.4 Reporting tools

1.3.5 Network and database administration tools

1.4 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.

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

2. **APPLICABILITY**: All county departments, employees, contractors, business partners, and volunteers must agree to this policy in writing upon onboarding and annually thereafter.

3. **VIOLATIONS**:

3.1 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.

3.2 County officials, county employees, contractors, consultants, temporary staff, and/or volunteers who engage in improper use of information technology and electronic communications under this policy are subject to disciplinary action, up to and including dismissal.

4. **GENERAL POLICY**:

4.1 Tillamook 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.

5. **POLICY**:

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

5.2 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 or telework

5.3 All computing and communications assets, including data, are property of Tillamook 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.

5.4 Personal devices (mobile phones, tablets, computers, etc..) may be allowed to connect to county resources and/or to conduct county business only by approval of the IS Director and an elected official or department head. Data and information on personal devices used for county business are subject to public records disclosure.

5.5 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.

5.6 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.

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

5.8 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.

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

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

5.11 No one other than IS 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.

5.12 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.

5.13 Personal use of electronic distribution groups is not allowed.

5.14 Software and Hardware

5.14.1 County owned, licensed, or subscribed computer software shall not be copied for personal use.

5.14.2 To minimize risk from data-destroying viruses, only software, hardware, services, and storage media owned, licensed, or subscribed by Tillamook 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 IS Director or designee.

5.14.3 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 IS 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.

5.14.4 Employees may not load privately owned, free, or shareware software on county systems or devices, nor connect (i.e. wired, wireless connection or by any other means) any privately owned device to a county system without county authorization, regardless of purpose.

5.14.5 Internet games, personal games, and internet gambling sites may not be used or accessed except as authorized for work purposes.

5.14.6 Accessing personal email, webmail, and cloud storage on county computers for personal or county business is prohibited, unless approved by the IS Director and an elected official or department head.

5.15 Email:

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

5.15.2 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.

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

5.15.4 All email communications are subject to inspection at any time without notice by the county. An elected official or department head may, with approval from HR or the County Counsel, request the IS Department to implement software to limit, restrict, and/or monitor employee Email usage at any time and without notice.

5.15.5 Mass distribution groups may only be used for official county business. department or county-wide e-mail groups and/or messages require authorization from the IS Department and the Board of Commissioners' Office. Events which mix county and personal business, such as charitable drives, employee retirements, or celebrations may be published with Board of Commissioners' Office authorization.

5.15.6 Responses to mass distribution emails shall be directed to the sender and/or specifically relevant parties only.

5.16 Instant Messaging

5.16.1 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.

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

5.16.3 Inappropriate use or communications using Instant messaging or similar function on county devices may be subject to disciplinary or performance management actions.

5.16.4 Instant messages will be logged and retained in accordance with Oregon Administrative Rules (OARs) and county retention policy.

5.16.5 All instant message communications are subject to inspection at any time without notice. An elected official or department head may, with approval from HR or the County Counsel, request the IS Department to implement software to limit, restrict, and/or monitor employee instant message usage at any time and without notice.

5.16.6 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.

5.17 Internet

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

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

5.17.3 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.

5.17.4 Elected officials and department heads in coordination with HR may establish more restrictive Internet use policies for their departments.

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

5.17.6 Use of internet email is subject to the standards outlined in Section 8.15 of this policy.

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

5.17.7.1 Defamatory, derogatory, insulting, or degrading material or information

5.17.7.2 Confidential, restricted, or privileged information

5.17.7.3 Copyrighted materials without the express consent of the copyright holder

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

5.17.9 Transmission of confidential or restricted information (HIPAA, CJIS, PII, etc..) via the Internet/Intranet requires authorization by the department head or elected official in conjunction with the IS Director. Confidential or restricted information approved for such transmission must be encrypted. Other approved methods to transmit confidential or restricted information include the following:

5.17.9.1 County approved secure cloud storage

5.17.9.2 County approved encrypted flash media (thumb drive, USB drive, etc....)

5.17.9.3 County approved encrypted CD/DVD media

5.17.10 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 IS Director prior to purchase. As assigned, employees may be responsible for monitoring proper use of these subscription services.

5.17.11 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.

5.17.12 When in a Tillamook County facility, personal devices may only connect to the Tillamook County Guest Wi-Fi network (Public201).

5.18 Passwords

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

5.18.2 Employees must disclose their passwords to their supervisor or manager upon request for any system having passwords which cannot be reset by IS 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.

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

5.18.4 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.

5.18.5 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.

5.18.6 HR or County Counsel 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.

5.18.7 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.

5.19 Encryption

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

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

5.20 Access to Electronic Files

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

5.20.2 The HR and/or County Counsel 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.

5.21 Telephones and Cell Phones

5.21.1 Employees shall not make personal long-distance telephone calls on land-line county phones.

5.21.2 Personal telephone calls, text and email messages (outgoing and incoming), within reason, are permitted, for limited duration, during the course of an employee's duties. Use of the cellular telephone or data device for threatening, harassing or communications of an inappropriate nature are not permitted, and are in violation of this policy. Inappropriate use of county cell phones may be subject to disciplinary action. Inappropriate use includes, but is not limited to, extensive personal use, engaging in communications in conflict or in violation of this policy, deleting public records, etc. Employees are on notice that common sense use of a county communication device applies towards consideration for appropriate use.

5.22 Remote Access

5.22.1 Remote access to county systems and/or data via county webmail or Virtual Private Network (VPN) may be granted upon request through a county remote access agreement.

5.22.2 When teleworking/working remotely all data electronic or paper, must be secured, stored, or destroyed in an appropriate manner, connection to external printers and/or external printing is authorized by exception only by request from the department head or as authorized for telework.

5.22.3 You are responsible to secure all county data both electronic and paper in nature. county computing systems and data must not be left unsecured or unattended without appropriate controls.

5.22.3.1 Computing systems and county data should never be left unattended in vehicles, computing systems and/or county data may be left for short periods of time in a locked trunk, but never overnight.

5.22.3.2 Unless authorized specifically in a telework agreement or by a department head, computing systems and county data should never be left unattended and unlocked non password protected state or in an accessible use condition outside of the county facilities. Computing systems and county data should never be left unattended in a hotel or similar unless all external doors are locked/secured.

5.23 Social Media

5.23.1 Social media usage is a use of information technology. As such, use of social media during work hours or using county systems including county-issued cellular devices and personal cellular devices approved for utilization for work purposes must comply with the county Social Media Policy, Mobile Devices Standard, and this policy

5.23.2 When posting on social media for non-work purposes, employees may not use their county job title, email address or other information showing county affiliation in a way that indicates they are acting as county employees or on the behalf of the county.

ADMINISTRATIVE POLICY

SECTION: Information Services	Policy: IS-2	
TITLE: Cyber Security Policy	ORDER #: 21-057	
DEPT: Information Services		
ADOPTED: 10/27/2021	REVIEWED: TBD	REVISED: TBD

1. **PURPOSE/OBJECTIVE:**

1.1 Tillamook County recognizes that information and the protection of information is required to serve our citizens. We seek to ensure that appropriate measures are implemented to protect our citizens information. This Cybersecurity Policy is designed to establish a foundation for an organizational culture of security.

1.2 The purpose of this policy is to clearly communicate Tillamook County's cyber security objectives and guidelines to minimize the risk of internal and external threats while taking advantage of opportunities that promote our objectives

1.3 This policy shall be reviewed annually to ensure that this document meets or exceeds all security requirements placed on the county from internal and external sources.

2. **APLICABILITY:** This policy applies to all county elected officials, employees, contractors, consultants, and others specifically authorized to access information and associated assets owned, operated, controlled, or managed by Tillamook County. Additionally, leadership must ensure that all contracts and similar agreements with business partners and service providers incorporate appropriate elements of this policy. Exceptions to this policy may be granted as provided herein and by operational need.

3. **VIOLATIONS:**

3.1 County officials, county employees, contractors, consultants, temporary staff, and/or volunteers who engage in improper use of information technology and electronic communications under this policy are subject to disciplinary action, up to and including dismissal.

4. **GENERAL POLICY**:

4.1 Tillamook County recognizes that information and the protection of information is required to serve our citizens. The county seeks to ensure that appropriate

measures are implemented to protect our citizens information. This Cybersecurity Policy is designed to establish a foundation for an organizational culture of security.

5. **POLICY:**

5.1 This policy aligns with Tillamook County General Administration Policy GA-2, Continuity of Operations and as necessary other Federal, State, and Local Emergency Management guidelines.

5.2 Oregon Public entities must comply with the Oregon Identity Theft Protection Act, ORS 646A.600 – 628. ORS 646A.622 (d) requires the implementation of a Cybersecurity program.

5.3 Non-compliance with this policy may pose risks to the organization; accordingly, compliance with this program is mandatory. Failure to comply may result in failure to obtain organizational objectives, legal action, fines, and penalties.

5.4 Breaches with the potential to impact more than 250 individuals must be reported to the Oregon Department of Justice.

IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER

5.5 The following sections outline Tillamook County's requirements and minimum standards to facilitate the secure use of organizational information systems. The information presented in this policy follows the format of the control families outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST CSF): Identify, Protect, Detect, Respond, and Recover.

5.6 The scope of security controls addressed in this policy focus on the activities most relevant to Tillamook County as defined by the Center for Internet Security (CIS) and industry best practices. Questions related to the interpretation and implementation of the requirements outlined in this policy should be directed to the IS Director.

IDENTIFY (ID)

6.1 Objective: To develop the organization's understanding that's necessary to manage cybersecurity risk to systems, people, assets, data, and capabilities.

6.2 Asset Management

6.2.1 An inventory of all approved hardware and software on Tillamook County network and systems will be maintained in a computer program or spreadsheet that documents the following:

6.2.1.1 The employee in possession of the hardware or software

6.2.1.1.1 Serial number
6.2.1.1.2 Type of device and description
6.2.1.1.3 A listing of software or devices that have been restricted

6.3 Data Protection

6.3.1 All employees are required to store sensitive, confidential, and critical files on servers.

6.3.1.1 All computer printouts should be printed, distributed, and stored in a manner that is commensurate with its confidentiality.

6.4 Personally Identifiable Information (PII)

6.4.1 An inventory of all PII information by type and location will be taken. The following table may be useful to inventory PPI.

Location	PII by type	Essential	Location	Owner
Website				
Contractors				
File in staff office				
File in building				
File offsite				
Desktop				
HR System				
Financial System				
Laptop				
Flash drive				
Cell phones				
Tablets				
Other				

6.4.2 Each manager will determine if PII is essential. If PII is not essential, it will either not be collected, or (if collected) will be destroyed. Do not collect sensitive information, such as a Social Security numbers, if there is no legitimate business need. If this information does serve a need, apply Tillamook County's record retention plan that outlines what information must be kept, and dispose of it securely once it is no longer required to maintain.

6.4.3 All PII no longer needed shall be shredded if in paper form or destroyed by IT if in electronic form.

6.4.4 The Oregon Identity Theft Protection Act prohibits anyone (individual, private or public corporation, government, or business) who maintains Social Security numbers from:

6.4.4.1 Printing a consumer's SSN on any mailed materials not requested by the consumer unless redacted

6.4.4.2 Printing a consumer's SSN on a card used by the consumer that is required to access products or services

6.4.4.3 Publicly posting or displaying a consumer's SSN, such as on a website

6.4.5 Exceptions include requirements by state or federal laws, including records (such as W2s, W4s, 1099s, etc.) that are required by law to be made available to the public, for use for internal verification or administrative processes, or for enforcing a judgment or court order. However, electronic transmittal of documents must include redaction of social security information.

PROTECT (PR)

6.5 Objective: To develop and implement appropriate safeguards to ensure the delivery of critical services.

6.5.1 Identity Management, Authentication and Access Control

6.5.2 IS Director, or designated as assigned, is responsible for ensuring that access to the organization's systems and data is appropriately controlled. All systems housing Tillamook County data (including laptops, desktops, tablets, and cell phones) are required to be protected with a password or other form of authentication. Except for the instances noted in this policy, users with access to county systems and data are not to share passwords with other employees unless at the direction of a supervisor or manager. (*See also Policy IS-1, Passwords)*

6.5.3 Tillamook County has established following the password configuration requirements for all systems and applications (where applicable): (See Attachment IS-1.1 Password Standards)

6.5.4 Other potential safeguards include:

6.5.4.1 Not allowing PII on mobile storage media

6.5.4.2 Locking file cabinets

6.5.4.3 Not allowing PII left on desktops

6.5.4.4 Encrypting sensitive files on computers

6.5.4.5 Requiring password protection

6.5.4.6 Implementing the record retention plan and destroying records no longer required

6.5.5 Where possible, multi-factor authentication will be used when users authenticate to the organization's systems.

6.5.5.1 Users are granted access only to the system data and functionality necessary for their job responsibilities.

6.5.5.2 Privileged and administrative access is limited to authorized users who require escalated access for their job responsibilities and where possible will have two accounts: one for administrator functions and a standard account for day-to-day activities.

6.5.5.3 All user access requests must be approved by requestor supervisor, system owner, and/or IT Manager.

6.5.5.4 It is the responsibility of the employee's supervisor to ensure that all employees and contractors who separate from the organization have all system access removed within 10 business days.

6.5.6 On an annual basis, a review of user and administrative access will be conducted under the direction of IS Director to confirm compliance with the access control policies outlined above.

6.5.7 On an annual basis, a review of badged users access to county facilities and resources will be conducted under the direction of the IS Director

6.6 Awareness and Training

6.6.1 Tillamook County personnel are required to participate in security training in the following instances:

6.6.1.1 All new hires are required to review and complete Use of Computing and Communications Assets awareness training in a timely manner as directed.

6.6.1.2 Formal security awareness refresher training is conducted monthly and annually. All employees are required to participate in and complete this training.

6.6.2 Workforce members will review and sign the Use of Computing and Communications Assets Policy annually.

6.6.3 On a periodic, but not less than annual basis, Tillamook County will conduct email phishing exercises of its users. The purpose of these tests is to help educate users on common phishing scenarios. It will assess their level of

awareness and comprehension of phishing, understanding and compliance with policy around safe handling of e-mails containing links and/or attachments, and their ability to recognize a questionable or fraudulent message.

6.7 Data Security

6.7.1 Data Classification

6.7.1.1 You must adhere to your Records Retention Policy regarding the storage and destruction of data. Data residing on county systems must be continually evaluated and classified into the following categories:

6.7.1.1.1 **Employees Personal Use:** Includes individual user's personal data, emails, documents, etc. This policy excludes an employee's personal information, so no further guidelines apply.

6.7.1.1.2 **Marketing or Informational Material**: Includes already-released marketing material, commonly known information, data freely available to the public, etc. There are no requirements for public information.

6.7.1.1.3 **Operational**: Includes data for basic organizational operations, communications with vendors, employees, etc. (non-confidential). Most data will fall into this category.

6.7.1.1.4 **Confidential:** Any information deemed confidential. The following list provides guidelines on what type of information is typically considered confidential. Confidential data may include:

6.7.1.1.4.1 Employee or customer Social Security numbers or personally identifiable information (PII)
6.7.1.1.4.2 Personnel files
6.7.1.1.4.3 Medical and healthcare information
6.7.1.1.4.4 Protected Health Information (PHI)
6.7.1.1.4.5 Network diagrams and security configurations
6.7.1.1.4.6 Communications regarding legal matters
6.7.1.1.4.7 Passwords/passphrases
6.7.1.1.4.8 Bank account information and routing numbers
6.7.1.1.4.9 Payroll information
6.7.1.1.4.10 Credit card information
6.7.1.1.4.11 Any confidential data held for a third party (be sure to adhere to any confidential data agreement covering such information)

6.7.2 Data Storage

6.7.2.1 The following guidelines apply to storage of the different types of organizational data:

6.7.2.1.1 **Operational**: Operational data should be stored on a server that gets the most frequent backups (refer to the Backup Policy for additional information). Some type of system- or disk-level redundancy is encouraged.

6.7.2.1.2 **Confidential**: Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard or code secured.

6.7.3 Data Transmission

6.7.3.1 The following guidelines apply to the transmission of the different types of organizational data.

6.7.3.1.1 **Confidential:** Confidential data must not be 1) transmitted outside the organization's network without the use of strong encryption, 2) left on voicemail systems, either inside or outside the organization's network.

6.7.4 Data Destruction

6.7.4.1 You must follow county or applicable State records retention policy before destroying data.

6.7.4.1.1 **Confidential:** Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

6.7.4.1.1.1 Paper/documents: Cross-cut shredding is required.

6.7.4.1.1.2 Storage media (CD's, DVD's): Physical destruction is required.

6.7.4.1.1.3 Hard drives/systems/mobile storage media: At a minimum, data wiping must be used. Simply reformatting a drive does not make the data unrecoverable. If wiping is used, the county must use the most secure commercially available methods for data wiping. Alternatively, the organization has the option of physically destroying the storage media.

6.7.5 Data Storage

6.7.5.1 Stored Data includes any data located on county-owned or county-provided systems, devices, media, etc. Examples of encryption options for stored data include:

6.7.5.1.1 Whole disk encryption

6.7.5.1.2 Encryption of partitions/files

6.7.5.1.3 Encryption of disk drives

6.7.5.1.4 Encryption of personal storage media/USB drives

6.7.5.1.5 Encryption of backups

6.7.5.1.6 Encryption of data generated by applications

6.7.5.2 Data while transmitted includes any data sent across the county network or any data sent to or from an county-owned or county-provided system. Types of transmitted data that shall be encrypted include:

6.7.5.2.1 VPN tunnels
6.7.5.2.2 Remote access sessions
6.7.5.2.3 Web applications
6.7.5.2.4 Email and email attachments
6.7.5.2.5 Remote desktop access
6.7.5.2.6 Communications with applications/databases

6.8 Information Protection Processes and Procedures

6.8.1 Secure Software Development

6.8.1.1 Where applicable, all software development activities performed by Tillamook County or by vendors on behalf of the county shall employ secure coding practices including those outlined below:

6.8.1.1.1 A minimum of three software environments for the development of software systems should be available – development, quality assurance/test, and a production environment. Software developers or programmers are required to develop in the development environment and promote objects into the quality assurance/test and production environments. The quality assurance/test environment is used for assurance testing by the end user and the developer. The production environment should be used solely by the end user for production data and applications. Compiling objects and the source code is not allowed in the production environment. The IS Director or an independent peer review will be required for promotion objects into the production environment.
6.8.1.1.2 All production changes must be approved before being promoted to production.
6.8.1.1.3 Developers should not have the ability to move their own code.
6.8.1.1.4 All production changes must have a corresponding help desk change request number.
6.8.1.1.5 Production changes should when feasible be developed in the development environment and tested for quality assurance.
6.8.1.1.6 All emergency changes must be adequately documented and approved.
6.8.1.1.7 Software code approved for promotion will be uploaded by IS Director to the production environment from the quality assurance environment once the change request is approved. The IS Director may work with the developer to ensure proper placement of objects into production.

6.8.2 Contingency Planning

6.8.2.1 The county's business contingency capability is based upon cloud and local backups of all critical business data. Full data backups will be performed on a weekly basis. Confirmation that backups were performed successfully will be conducted daily. Testing of cloud backups and restoration capability will be performed on as needed or yearly basis.

6.8.2.2 During a contingency event, all IT decisions and activities will be coordinated through and under the direction of the IS Director.

6.8.2.3 The following business contingency scenarios have been identified along with the intended responses:

6.8.2.3.1 In the event that one or more of Tillamook County 's systems or applications are deemed corrupted or inaccessible, the IS Director and system owner will work with the respective vendor(s) to restore data from the most recent cloud or local backup and, if necessary, acquire replacement hardware.

6.8.2.3.2 In the event that the location housing the Tillamook County systems are no longer accessible, the IS Director will work with the respective vendor(s) to acquire any necessary replacement hardware and software, implement these at one of the organization's other sites, and restore data from the most recent cloud or local backup.

6.8.3 Network Infrastructure

6.8.3.1 Tillamook County will protect the county electronic communications network from the Internet by utilizing a firewall. For maximum protection, the corporate network devices shall meet the following configuration standards:

6.8.3.1.1 Vendor recommended, and industry standard configurations will be used.

6.8.3.1.2 The IS Director and Systems Manager will follow a two-person integrity model to approve and implement changes to critical systems i.e. Firewall, Router, and/or switches.

6.8.3.1.3 Router, firewall, and switch passwords must be secured and difficult to guess.

6.8.3.1.4 The default policy for the firewall for handling inbound traffic should be to deny all and permit by approved exception only.

6.8.3.1.5 Inbound traffic containing ICMP (Internet Control Message Protocol) traffic should not be passed in from the Internet, or from any un-trusted external network.

6.8.3.1.6 All web services running on routers must be disabled.

6.8.3.1.7 Simple Network Management Protocol (SNMP) Community Strings must be changed from the default "public" and "private".

6.9 Network Server

6.9.1 Servers typically accept connections from several sources, both internal and external. As a rule, the more sources that connect to a system, the more risk

associated with that system, so it is particularly important to secure network servers. The following statements apply to the organization's use of network servers

6.9.1.1 Unnecessary files, services, and ports should be removed or blocked. If possible, follow a server-hardening guide, which is available from the leading operating system manufacturers.

6.9.1.2 Network servers, even those meant to accept public connections, must be protected by a firewall or access control list.

6.9.1.3 If possible, a standard installation process should be developed for the county's network servers. A standard process will provide consistency across servers no matter what employee or contractor handles the installation.

6.9.1.4 Clocks on network servers should be synchronized with the county's other networking hardware using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.

6.9.2 Network Segmentation

6.9.2.1 Network segmentation is used to limit access to data within the Tillamook County network based upon data sensitivity. Tillamook County maintains two wireless networks. The guest (Public201) wireless network is password protected, and proper authentication will grant the user internet access only. Access to the secure wireless (Private 201) network is limited to Tillamook County personnel and provides the user access to the intranet.

6.9.3 Protective Technology

6.9.3.1 Email Filtering, A good way to mitigate email related risk is to filter it before it reaches the user so that the user receives only safe, business-related messages. Tillamook County will filter email at the Internet gateway and/or the mail server. This filtering will help reduce spam, viruses, or other messages that may be deemed either contrary to this policy or a potential risk to the organization's IT security.

6.9.3.1.1 Additionally, technology may have been implemented to identify and quarantine emails that are deemed suspicious. This functionality may or may not be used at the discretion of the IS Director

6.9.3.2 Network Vulnerability Assessments, On an annual basis, Tillamook County will perform both internal and external network vulnerability assessments. The purpose of these assessments is to establish a comprehensive view of the organization's network as it appears internally and externally. These evaluations will be conducted under the direction of IS Director to identify

weaknesses with the network configuration that could allow unauthorized and/or unsuspected access to the organization's data and systems.

6.9.3.2.1 As a rule, "penetration testing," which is the active exploitation of organization vulnerabilities, is discouraged. If penetration testing is performed, it must not negatively impact organization systems or data.

DETECT (DE)

6.10 Definition: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

6.10.1 Anomalies and Events

6.10.1.1 The following logging activities are conducted by IT SPEC I - VI under the direction of IS Director:

6.10.1.1.1 Domain Controllers - Active Directory event logs will be configured to log the following security events: account creation, escalation of privileges, and login failures.

6.10.1.1.2 Application Servers - Logs from application servers (e.g., web, email, database servers) will be configured to log the following events: errors, faults, and login failures.

6.10.1.1.3 Network Devices - Logs from network devices (e.g., firewalls, network switches, routers) will be configured to log the following events: errors, faults, and login failures.

6.10.1.2 Passwords when feasible should not be contained in logs.

6.10.1.3 Logs of the above events will be reviewed by IT SPEC I - VI at least once per month. Event logs will be configured to maintain record of the above events for a minimum three months.

6.10.2 Security Continuous Monitoring

6.10.2.1 Anti-Malware Tools

6.10.2.1.1 All county servers and workstations will utilize Windows Security to protect systems from malware and viruses. Real-time scanning will be enabled on all systems and weekly malware scans will be performed. A monthly review of the Windows Security dashboard will be conducted by IT SPEC I - VI to confirm the status of virus definition updates and scans.

6.10.2.1.2 Tillamook County utilizes appropriate security process and technology to protect mobile devices from malware and viruses.

6.10.3 Patch management

6.10.3.1 All software updates and patches will be distributed to all Tillamook County systems as follows:

6.10.3.1.1 Workstations will be configured to install software updates every week automatically.

6.10.3.1.2 Server software and critical infrastructure updates will be manually installed when feasible monthly.

6.10.3.1.3 Any exceptions shall be documented.

RESPOND (RS)

6.11 Definition: Develop and implement appropriate activities to act regarding a detected cybersecurity incident.

6.11.1 Response Planning

6.11.1.1 The county's annual security awareness training, which can be ongoing training, shall include direction and guidance for the types of security incidents users could encounter, what actions to take when an incident is suspected, and who is responsible for responding to an incident. A security incident, as it relates to the Tillamook County information assets, can be defined as either an Electronic or Physical Incident.

6.11.1.2 The IS Director is responsible for coordinating all activities during a significant incident, including notification and communication activities. They are also responsible for the chain of escalation and deciding if/when outside agencies, such as law enforcement, need to be contacted.

6.11.2 Information Technology Incidents

6.11.2.1 This type of incident can range from an attacker or user accessing the network for unauthorized/malicious purposes to a virus outbreak or a suspected Trojan or malware infection. When an electronic incident is suspected, the steps below should be taken in order.

6.11.2.1.1 Remove the compromised device from the network by unplugging or disabling network connection. Do not power down the machine.

6.11.2.1.2 Report the incident to the IS Director or IT SPEC VI, Systems Manager.

6.11.2.1.3 Notify County Counsel, Insurance Carrier, Breach Coach, and retained third-party service provider (and/or computer forensic specialist) as needed.

6.11.2.2 The remaining steps should be conducted with the assistance of the third-party IT service provider and/or computer forensics specialist.

6.11.2.2.1 Obtain third-party incident play book / best business practices, assess it against the current situation for recommendations and actions
6.11.2.2.2 Disable the compromised account(s) as appropriate.
6.11.2.2.3 Backup all data and logs on the machine, or copy/image the machine to another system.
6.11.2.2.4 Determine exactly what happened and the scope of the incident.
6.11.2.2.5 Determine how the attacker gained access and disable it.
6.11.2.2.6 Rebuild the system, including a complete operating system reinstall.
6.11.2.2.7 Restore any needed data from the last known good backup and put the system back online.
6.11.2.2.8 Take actions, as possible, to ensure that the vulnerability will not reappear.
6.11.2.2.9 Conduct a post-incident evaluation. What can be learned? What could be done differently?
6.11.2.2.10 Document timeline, key events, key actions, and costs as able

6.11.3 Physical Incidents

6.11.3.1 A physical security incident involves the loss or theft of a laptop, mobile device, PDA/Smartphone, portable storage device, or other digital apparatus that may contain organization information. All instances of a suspected physical security incident should be reported immediately to the IS Director and/or Sheriff's Office.

6.11.4 Notification

6.11.4.1 Incidents suspected of resulting in the loss of third-party/customer data, require immediate County Counsel notification.

6.11.4.1.1 County Counsel will determine if it is appropriate to contact the county's risk management carrier claims department.
6.11.4.1.2 County Counsel will work with the county's risk management carrier and the Breach Coach to assess notification compliance requirements https://justice.oregon.gov/consumer/DataBreach/Home/Submit

RECOVER (RC)

6.12 Recovery processes and procedures are executed and maintained to ensure timely restoration of systems and/or assets affected by cybersecurity events.

6.13 Tillamook County's cyber policy, legal services, and other retained services well be reviewed annually for relevance and accuracy.

6.14 The IS Director is responsible for managing and directing activities during an incident, including the recovery steps.

6.15 Recovery planning and processes are improved by incorporating lessons learned into future activities.

6.16 Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet service providers, owners of the affected systems, victims, and vendors.

6.17 External communications should only be handled by designated individuals at the direction of Board of Commissioners. Recovery activities are communicated to internal stakeholders, executives, and management teams.

ADMINISTRATIVE POLICY

SECTION: Information Services		POLICY: IS-3
TITLE: Cellular Telephones and Data Devices Usage		ORDER #: 21-057
DEPT: Information Services		
ADOPTED: 10/27/2021	REVIEWED: TBD	REVISED: TBD

1. **PURPOSE/OBJECTIVE:**

1.1 To establish the issuance, usage, and accountability of cellular telephones and data devices for county business use. The policy outlines the cellular telephone and data device options supported by Tillamook County, appropriate use restrictions, and other administrative issues relating to cellular telephone and data device acquisition and reimbursement. This policy is established to enhance employee safety, limit county liability, ensure appropriate customer service, and manage telecommunications costs.

2. **APPLICABILITY:**

2.1 All county departments, officials, employees, contractors, business partners, and volunteers

3. **VIOLATIONS:**

3.1 The proper use of cellular telephones and data devices enhance productivity and allows the county to meet increased service needs. It is the responsibility of each county employee to use cellular telephones and data devices properly. It is the responsibility of each county official and department head to ensure this policy is enforced

3.2 County officials, county employees, contractors, consultants, temporary staff, and/or volunteers who engage in improper use of information technology and electronic communications under this policy are subject to disciplinary action, up to and including dismissal. Disciplinary actions are subject to applicable policy or collective bargaining agreement.

4. **GENERAL POLICY:**

This policy establishes guidelines for the use of county-assigned cellular telephones and data devices, i.e. Blackberry devices, Android, iPhone, tablets etc., (cellular device), in Tillamook County by all county officials, employees, and volunteers and for the reimbursement of business use of personal cellular telephone and data devices. It is the policy of Tillamook County that all county equipment be managed and used to

conduct the business of the county in a safe, efficient, and cost-effective manner. All departmental policies must meet the minimum standards set forth in this policy.

4.1 This policy will be reviewed by the Information Services (IS) Director and County Counsel every two years and updated as needed.

4.2 All communications using county cellular telephones or data devices – verbal, written or other – must meet professional standards of conduct. Such standards of conduct include common sense uses that the reasonable public would deem are inappropriate, including but not limited to conducting personal business not related to county duties; excessive and/or inappropriate personal use; accessing, displaying, or transmitting images or content of a sexual or pornographic nature, engaging in unlawful conduct, communications in violation of county policy including sexual harassment, workplace violence and bullying.

4.3 Employees may use county supplied cellular telephones and data devices for any legitimate safety, security, or emergency purposes.

4.4 Employees shall not use county supplied cellular telephones and data devices for any illegal, disruptive, unethical, or unprofessional activities, or for personal gain, or for any purpose that would jeopardize the legitimate interests of Tillamook County.

5. **POLICY GUIDELINES:**

5.1 DEFINITIONS:

5.1.1 Cellular Telephone Device: is a device that can make and receive telephone calls over a secure link while moving around a wide geographic area. It does so by connecting to a cellular network provided by a mobile telephone service provider, allowing access to the public telephone network. This device may also be capable of connecting to data network features if the cellular telephone has an integrated data plan.

5.1.2 Cellular Data Device: is a device that connects to a cellular network for access to the internet for data transmission, but does not make or receive telephone calls, e.g., iPads, Laptops, Mobile Data Terminal (MDTs).

5.1.3 Activating: is the process of making a cellular or data device connected to a cellular network via a contractual arrangement for services via a cellular vendor.

5.1.4 Deactivating: is the process of discontinuing the cellular service or connection to a cellular network via a cellular vendor.

5.1.5 Cellular Data Plan: an agreement with a cellular vendor to provide data device connectivity via a cellular network. (May also be referred to as a usage plan or data allowance.)

5.2 RESPONSIBILITIES

5.2.1 Cellular telephone and data devices shall be assigned at the direction of an elected official or department head. Department heads and elected officials are responsible for determining if a valid business reason exists to assign a cellular telephone and/or data device. Valid business reasons include:

5.2.1.1 Departmental requirements indicate utilizing a cellular telephone and/or data device is an integral part of performing duties of the job description.

5.2.1.2 More than 30% of the employee's job duties are performed in the field

5.2.1.3 The employee is a critical decision maker, or has unique technical expertise

5.2.1.4 The employee is required to be on-call outside of normal work hours as a function of his or her job

5.2.1.5 Official duties expose the employee to danger

5.2.1.6 Cellular telephone and data devices will not be issued to student workers, contract employees, temporary employees, consultants, or other workers that do not have a compelling use for this equipment.

5.2.2 It is against Tillamook County policy to provide a cellular telephone device or data device to promote morale or good will, to attract a prospective employee or as a means of providing additional compensation to an employee.

5.2.3 This equipment is county property and is to be maintained in good condition and working order. If a county-owned cellular telephone or data device is damaged, lost or stolen, the employee must immediately notify his or her supervisor and the IS Department.

5.2.3.1 Personal telephone calls, text and email messages (outgoing and incoming), within reason, are permitted, for limited duration, during the course of an employee's duties. Use of the cellular telephone or data device for threatening, harassing or communications of an inappropriate nature are not permitted, and are in violation of this policy. Inappropriate use of county cell phones may be subject to disciplinary action. Inappropriate use includes, but is not limited to, extensive personal use, engaging in communications in conflict or in violation of this policy, deleting public records, etc. Employees are on notice that common sense use of a county communication device applies towards consideration for appropriate use.

5.2.4 An assigned cellular telephone and/or data device will remain on the cellular telephone or data device plan provided by the county as established by the IS Department.

5.2.5 All employees and elected officials receiving a cellular telephone, reimbursement for county use of a cellular telephone and/or a data device will complete and submit a "Cellular Telephone and Data Device End User Agreement."

5.2.6 Some cellular telephones and data devices need to be regularly backed up and maintained. For those devices that do require a backup, the only acceptable method is to use a county workstation or laptop as a target device for the backup and maintenance process. It is strictly prohibited to back up a county-owned cellular telephone or data device to a non-county workstation, laptop, or device.

5.2.7 Use of a cellular telephone or data device to capture images, video, or audio, whether built into the device or through a third-party application, is strictly prohibited in the workplace, unless required as a function of the employee's position. Usage of a cellular telephone or data devices to capture images, video or audio is prohibited in restrooms.

5.2.8 Departments having employees who have infrequent needs for access to a cellular telephone may establish a "pool" phone that is available for use as needed. Examples of this situation include rotational "on-call" responsibilities for employees.

5.3 Personal Cellular Telephones and Data Devices:

5.3.1 For employees represented by AFSCME, personal cell phones and data devices will not be used for work purposes, except for an emergency or as authorized by a department head for an unexpected and very limited specific duration and purpose. Unauthorized use of personal cell phones and data devices for work purpose may lead to disciplinary action.

5.3.2 Employees are on notice that personal use of cell phones and data devices for work purposes are subject to public records disclosure as applicable under law as well as access by the county limited to those work purposes.

5.4 Tillamook County will not provide employees an allowance or stipend for personal cellular telephone and or data device usage.

5.5 The MDM service is a full-featured mobile device management solution for securing, monitoring, reporting on automating the management of mobile devices. Management includes configuring synchronization of email, contracts, and calendars, configuring Wi-Fi, VPN, bookmarks, and an enterprise app store.

5.5.1 IS will remove the containerized MDM suite upon HR notification of the employee's departure from county service.

5.5.2 Employee-owned Device Functionality and Feature Management:

5.5.2.1 Cameras in mobile devices are not to be used in organization's secured facility areas unless permission from site management is obtained beforehand.

5.5.2.2 Upon organization's request, users must allow the installation of a mobile device management software agent, or any other software deemed necessary, on the user's device.

5.5.2.3 The device functionality must not be modified unless required or recommended by county IS staff. The use of devices that are "jail broken", "rooted" or have been subjected to any other method of changing built-in protections is not permitted and constitutes a material breach of this policy.

5.5.2.4 Users must accept that, when connecting the employee-owned mobile device to county resources, county security policy will be enforced on the device. The security policy implemented may include, but is not limited to, areas such as passcode, passcode timeout, passcode complexity and encryption.

5.5.2.5 Users must take appropriate precautions to prevent others from obtaining access to their mobile device(s). Users will be responsible for all transactions made with their credentials, and should not share individually assigned passwords, PINs or other credentials.

5.5.2.6 Users are responsible for bringing or sending the mobile device to the IS Department and handing over necessary device access codes when notified that the device has been selected for a physical security audit, or in the event the device is needed for e-discovery purposes.

5.5.2.7 Users may not provide access credentials to any other individual, and each device in use must be explicitly granted access after agreeing to the terms and conditions of this document.

5.5.3 IS will remove the containerized MDM suite upon HR notification of the employee's departure from county service.

5.5.4 County IS staff will provide support and guidance for the installation and connection to county infrastructure and network resources. All other support-related issues must be directed to the mobile device service provider.

5.5.5 Use of personal cellular telephones and data devices (including social media, internet, text messages, and phone calls) during work hours:

5.5.5.1 The use of personal cellular telephones and data devices not owned by the county for business purposes should be limited to necessity during work time. Use of personal communication devices for work purposes may create a public record subject to public disclosure.

5.5.5.2 The use of personal cell phones or other personal communication devices for personal reasons during work hours is discouraged and should be limited to matters requiring immediate attention. As with any personal matter, employees are encouraged to use allotted lunch and breaks for these purposes. Notify your supervisor of any special circumstances which may require use outside of the recommended times.

5.5.5.3 Employees should not be engaged in continual texting, messaging, or similar repetitive conduct when using personal devices during work hours, unless on break or lunch periods.

5.6 Termination from the Program

5.6.1 The following scenarios may result in termination from the employee-owned mobile device program:

5.6.1.1 Tillamook County may cancel the program at any time, for any reason.

5.6.1.2 Users may withdraw from the program at any time and for any reason.

5.6.1.3 User violation of policy – disciplinary actions are subject to applicable policy or collective bargaining agreement.

5.6.1.4 Termination of employment will end the participation in the program.

5.6.2 Regardless of reason for the termination from the employee-owned mobile device program, the following process will occur:

5.6.2.1 County IS staff will remotely wipe all devices with organization's information on them. It will be up to the end user to back up personal application and data prior to this event, and to restore only personal information after the device has been cleared of contents.

5.6.2.2 Certain devices may be considered an exception; the help desk will verify that all organization related information has been removed.

5.6.2.3 Former or terminated employees are not authorized to restore any application or data that originated through the relationship with their former organization. Any attempt to restore such information will be subject to legal action against the former employee.

5.6.2.4 For non-represented terminated employees or those terminated under an MDM compliance agreement, employees must complete the termination agreement (Appendix 1) on having no other copies of Tillamook County information stored on employee-owned devices (or backups of them), regardless of media.

5.7 Safety: Oregon law prohibits drivers from talking on a cellular telephone while driving. County policy strongly discourages making or receiving cellular telephone calls on a hands-free device, except in an emergency. Use of a cellular telephone and/or data device includes activating or deactivating the telephone, dialing, answering, conversing, and sending or receiving email or text messages.

5.8 Privacy: Employees, volunteers, and officials should have no expectation of privacy as to any data, including voicemail, images and/or text messages, transmitted, stored, or received on county cellular telephones and data devices provided or paid for by the county. The county reserves the right to inspect such equipment, its contents, related data compilations, and Internet usage and resources as necessary for business purposes without prior notice to the employee and/or in the employee's absence. Personal passwords may be used, and the use of a password does not affect the county's ownership of the electronic information or the right to inspect such information. Employees are required to provide all passwords to the relevant department head, if requested, and the county may override said passwords. Any data transmitted, stored, or received on county cellular telephones and data devices provided or paid for by the county may be subject to the Public Information Act.

5.9 Cellular telephone and data device etiquette:

5.9.1 Cell phones and other devices can be a distraction in the workplace. Personal cellular telephones and data devices not in use for approved county business should be turned off or in vibrate or silent mode during work hours. To ensure the effectiveness of meetings, employees are asked to place their county and Personal cellular telephones and data devices in "silent" or "vibrate'. Employees should refrain from constant viewing of their devices for text messages or similar notices, unless justified by operational needs.

5.9.2 When making cellular telephone calls, ensure your communication is made in a location or manner that is not disruptive to other county employees.

5.9.3 Cellular telephone calls and communication should be conducted to not compromise confidential data privacy.

5.10 Annual Report: The IS Department will prepare an annual report to the board.

ADMINISTRATIVE POLICY

SECTION: Information Services	POLICY: IS-4	
TITLE: County Social Media Accounts Policy	ORDER #: 21-057	
DEPT: Information Services		
ADOPTED: 10/27/2021	REVIEWED: TBD	REVISED: TBD

1. **PURPOSE/OBJECTIVE:**

1.1 To address the fast-changing landscape of the Internet and the way residents communicate and obtain information online, county departments may consider using social media platforms to reach a broader audience. The county encourages the use of approved social media forums and accounts of behalf of representing the County to further the goals of the county and the missions of its departments, where appropriate.

1.2 The Tillamook 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

1.3 The Tillamook 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.

1.4 The Tillamook County Administrative Policies and Procedures manual of the Tillamook 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.

2. **APPLICABILITY:**

2.1 All county departments, officials, employees, contractors, business partners, and volunteers

3. **EXCEPTIONS:**

3.1 Exceptions to this policy will be approved by the Board of Commissioners or designee.

3.1.1 The following criteria will be used to determine approval of an exception:

3.1.1.1 The exception request is driven by the needs of the department making the request or would benefit the department making the request in a manner that is particularly relevant to the function served by that department.

3.1.1.2 The exception will not compromise the county's ability to control the content that appears on county social media accounts; and

3.1.1.3 The exception will not compromise the county's compliance with state or federal law, including Oregon public records laws.

3.1.1.4 Exception requests must be submitted to the Board of Commissioners or designee at least seven working days prior to the requested start date.

3.1.1.5 Approvals of exceptions will be sent to IS Department.

4. **VIOLATIONS:**

4.1 The proper use of social media on or behalf of county purposes enhances productivity and allows the county to meet increased service needs. It is the responsibility of each county employee to use social media properly. It is the responsibility of each county official and department head to ensure this policy is enforced.

4.2 County officials, county employees, contractors, consultants, temporary staff, and/or volunteers who engage in improper use of information technology and electronic communications under this policy are subject to disciplinary action, up to and including dismissal. Disciplinary actions are subject to applicable policy or collective bargaining agreement.

5. **GENERAL POLICY:**

5.1 The county has an overriding interest and expectation in deciding what is "spoken" on behalf of the county on social media. This policy establishes guidelines for the use of social media platforms.

5.2 This policy will be reviewed by the Information Services (IS) Director and County Counsel every two years and updated as needed.

6. **POLICY GUIDLINES:**

6.1 The county's website (www.co.tillamook.or.us) will remain the county's primary and predominant Internet presence.

6.1.1 County social media accounts are to be used for the following purposes:

6.1.1.1 As channels for disseminating time-sensitive information as quickly as possible (example: emergency information); and

6.1.1.2 As marketing/promotional channels that increase the county's ability to broadcast its messages to the widest possible audience.

6.1.2 County social media accounts and the official county website should work cooperatively to convey information to the public about county programs and services. Whenever practicable, content posted on county social media accounts shall contain links directing users back to the county's official website for in-depth information, forms, documents, or online services necessary to conduct business with the county.

6.1.3 County social media accounts are not for personal use and are solely to conduct county business within the scope of each individuals work duties, positions or function. Use of county social media accounts are to reflect the business purposes of the county. Employees are not to engage in personal commentary, opinions, or related when using county social media accounts.

6.2 County departments must receive approval from the Board of Commissioners, or designee, before establishing a new account on any social media platform. Before establishing a new account on any social media platform, a county department must develop (a) Administrative Standards (Attachment 1) and (b) Operational Guidelines (Attachment 2). These documents along with an IS Risk Assessment Statement shall be provided to the Board of Commissioners or designee, in order to receive approval.

6.2.1 Departments that already operate social media accounts at the time of the adoption of this policy to obtain approval may continue operating those specific accounts. Such departments must, however, comply with Section 6.2.2 below.

6.2.2 County departments that already operate social media accounts shall develop the Administrative Standards and Operational Guidelines discussed in Section 6.2 within 90 days of the adoption of this policy.

6.2.3 The department head of each department that operates social media accounts, or a designee, must review the Social Media Standards (Attachment 1) and Social Media Operational Guidelines (Attachment 2) adopted by that department at least annually and provide certification to the IS Department of review. Information contained within these documents must be revised at this time if the department's use of social media has changed or if the employees with access to county social media accounts have changed. The department head, or designee, shall notify the Board of Commissioners, or designee, of any revisions.

6.3 County social media accounts will be assessed annually for compliance to county policy.

6.4 The elected official or department head of each department that operates social media accounts is ultimately responsible for any content posted on social media accounts operated by that department.

6.4.1 The department head, or a designee, must be assigned account privileges for the purpose of accessing social media accounts operated by that department.

6.4.2 If the head of a county department appoints a designee to oversee that department's social media accounts, that department head remains ultimately responsible for all content appearing on that social media account.

6.5 All county social media content, including comments from members of the public and other content provided by persons not employed by the county, shall comply with the moderation guidelines adopted by the county.

6.6 County social media content shall comply with all appropriate county policies and standards

6.7 In general, county social media accounts shall be maintained and operated by county employees. Exceptions may be granted when good cause exists to allow contractors or volunteers to operate county social media accounts.

6.8 County social media content shall comply with county and state ethics and elections codes and administrative rules.

6.9 County social media content, including comments and other content provided by members of the public, is subject to State of Oregon public records laws. Any content maintained in a social media format that is related to county business, including but not limited to lists of subscribers and posted communication, is a public record. Each department that operates social media accounts is responsible for responding completely and accurately to any public records request for public records on social media. Content related to county business shall be maintained in an accessible format independent of the social media platform so that it can be produced in response to a request.

6.10 Oregon state law and relevant county records retention schedules apply to social media content. All departments that make use of social media platforms shall preserve records required to be maintained. The records retention shall be pursuant to a relevant records retention schedule for the required retention period in a format that preserves the integrity of the original record and is easily accessible. All materials posted on a social media platform, including comments and other content provided by persons not employed by the county, will also be retained in another medium.

6.11 The county will approach the use of social media tools, including design standards, as consistently as possible, enterprise wide.

6.12 Operational Guidelines:

6.13 Users and visitors to county social media accounts shall be notified that the intended purpose of the account is to engage with members of the public in a way that helps county departments carry out their intended functions. Members of the public may post comments or other content in a manner consistent with the county's moderation guidelines, but the county will not publicly display content that violates those guidelines. An appropriate email address should also be provided for persons that prefer to communicate with the department by email. The information described in this section may be made available by a link from the social media account.

6.14 The head of each department that operates a social media account, or a person designated by that department head, shall ensure that all content posted to social media accounts operated by that department complies with the following moderation guidelines:

6.14.1 Content and comments must be topically related to the services provided by the department that maintains the social media account.

6.14.2 Neither content provided by the county nor comments may contain profanity or abusive language.

6.14.3 County social media accounts shall not be used for purposes of harassment, discrimination, or similarly related conduct.

6.14.4 County social media accounts shall not be used to disseminate:

6.14.4.1 Content that promotes, fosters, or perpetuates discrimination on the basis of race, creed, color, age, religion, gender, marital status, status with regard to public assistance, national origin, physical or mental disability or sexual orientation.

6.14.4.2 Sexual content or links to sexual content.

6.14.4.3 Information that may tend to compromise the safety or security of the public or public systems.

6.14.4.4 Content that violates a legal ownership interest of any other party; or

6.14.4.5 Promotion or opposition of any person campaigning for election to a political office or promoting or opposing any ballot proposition.

6.14.5 County social media accounts shall not be used to solicit commerce.

6.14.6 County social media accounts shall not be used to conduct or encourage illegal activities.

6.14.7 County social media accounts shall not be used to disclose any information that the county and its employees must keep confidential by law or administrative rule.

6.14.8 A link to the moderation guidelines listed in section above shall be prominently featured on any social media account maintained by the county.

6.15 Content that does not comply with the moderation guidelines must not be publicly posted. It is, however, still a public record and copy must be retained.

6.16 Each county department with a social media presence shall maintain a list of all social media accounts operated by that department, including login and password information, and the names of any employees with access to county social media accounts. Each department will restrict access to social media accounts operated by that department to the department head or designee, and to employees chosen by the department head or designee whose job duties involve accessing department social media accounts. The department head or designee will update the list of employees with access to social media accounts operated by that department whenever an employee gains or loses access to department accounts.

6.16.1 County social media accounts will be operated by county employees. Departments wishing to allow contractors or volunteers to operate county social media accounts must apply for an exception under Section 9 of this policy. The department seeking the exception shall maintain a list of all volunteers or contractors with access to county social media accounts.

6.17 The Board of Commissioners authorizes the IS Director or designee to immediately edit or remove content from social media accounts that is deemed in violation of the social media policy, the moderation guidelines laid out in section 8.14 of this policy, or any applicable law.

6.18 The head of each department that operates a social media account, or a designee, shall review social media accounts operated by that department no less than annually. If a social media account has fallen into disuse or no longer provides a benefit to the department that operates the account, the department head or designee may order the account deactivated.

6.19 Photographs or video of county employees, contractors, and volunteers may be used on county social media accounts only with permission of the employee, contractor, or volunteer pictured; written permission is not necessary if the person depicted has been specifically notified that the photograph may be used on a county social media account and has been given the opportunity to move out-of-frame before the photograph is taken.

6.19.1 Photographs or video taken in a public place may be used on county social media accounts without obtaining permission from any person whose image or likeness may incidentally be contained in the photograph or video.

6.19.2 Photographs or video depicting any person other than a county employee, contractor, or volunteer in a closed or non-public setting may be used on county social media accounts only with written or email permission from the person depicted (see Attachment 3: Photography Consent Form).

6.19.3 Employees taking photographs or video that may be posted on county social media accounts must be aware at all times of the privacy or security concerns applicable to the location where the photographs or video is being taken. Care must be taken when taking photographs or video at or around Health Department, Sheriff's Office, and Juvenile Department facilities.

6.20 County social media accounts may only "Like", "Follow" or similarly express approval for social media accounts operated by the following:

6.20.1 Any other Tillamook County department.

6.20.2 The State of Oregon, or any component of Oregon state government.

6.20.3 The government of any Oregon county or city.

6.20.4 The government of any other state, or of any other city or county within the United States.

6.20.5 The United States federal government, or any component of the United States federal government.

6.20.6 Entities outside of government that have a well-established relationship with the county or with departments of the county, evidenced by participation in county initiatives and programs, or by actions of the Board of Commissioners.

6.21 For each social media platform approved for use by the county, the IS Department will develop the following documentation:

6.21.1 Technical standards and processes for using social media platforms, and

6.21.2 Enterprise-wide design standards.

Attachment 1

Tillamook County [Department]
Administrative Standards for Social Media Use for County Accounts

Tillamook County encourages work related use of social media to facilitate communication with constituents and sharing of information in support of the mission and business of Tillamook County and [Department].

Pursuant to Tillamook County Social Media Use Policy, Tillamook County departments engaging in social media must develop and adopt operational and administrative standards for social media use. Per policy guidelines, the county has an overriding interest and expectation in deciding what is spoken on behalf of the county on social media sites. Therefore, operational, and administrative standards must be reviewed and approved by the County Counsel, or designee, before a social media account is established for a department or division within a department.

The Tillamook County [Department] has developed and adopted the following administrative and operational standards for social media use. These operational and administrative standards are used in conjunction with Tillamook County Policy IS-4 Social Media Use Policy. Employees authorized to post content on behalf of [Department] understand and will comply with the following standards.

1. Pursuant to Policy IS-4, the head of [Department] is ultimately responsible for all content that appears on the social media accounts operated by [Department]. The head of [Department] further designates the following person to exercise administrative authority over the social media accounts operated by [Department]:

   _____

2. [Department] authorizes the following person(s) to communicate on behalf of the department on social media accounts(s):

   _____
   _____
   _____

3. [Department] intends to establish accounts on the following social media platform(s) to share information in support of the mission and business of the department:

   _____
   _____
   _____

4. [Department] recognizes that social media use is authorized for county/department business purposes and must comply with federal, state, and county laws, rules, and regulations, and county and department policies and procedures.

5. [Department] intends to update and maintain the accounts at _____ intervals.

6. Removal of the account or any of its contents may be determined by the department head or designee, IS Director, County Counsel, or Board of Commissioners.

Attachment 2

Tillamook County [Department]
Operational Standards for Social Media Use for County Accounts

Employees authorized to post content on social media accounts are required to:

1. Protect and respect the privacy of clients, partners, and other employees; notify bystanders when you are taking photographs or video for use on county social media and afford an opportunity for people to get out of frame; obtain written or email permission to use the image or likeness of any person when taking photographs or video in a closed or non-public setting; follow all relevant security and privacy policies when taking photographs or video at or near county facilities.

2. Comply with federal, state and county laws regarding public records, copyright, records retention, fair use, privacy, and financial disclosure laws.

3. Check facts, cite sources, avoid copyright infringement, acknowledge, and correct errors, and check spelling and grammar before making a post live on any social media site.

4. Post only within the employee's area of expertise and knowledge.

5. Make corrections expediently and note that a correction was made.

6. Maintain confidentiality of county information.

7. Follow the rules and procedures of any social media site on which they are posting content on behalf of Tillamook County.

8. Regularly maintain and update active department sites.

9. Follow department standards for identifying themselves when posting on a social media site.

10. Obtain department head approval before posting anything as an official statement of Tillamook County unless the employee is an authorized spokesperson, and the information is posted on the county/department's web site.

Employees authorized to post content on social media sites are prohibited from:

1. Making libelous and/or defamatory or false statements.

2. Plagiarizing material.

3. Sharing private, personal, or confidential information.

4. Posting commercial promotions or spam.

5. Posting information that is in draft form or is pending publication.

6. Including content in postings for which the county does not own the copyright or does not have legal permission to use.

7. Posting comments in support or opposition of political campaigns or ballot measures. Employees who engage in improper use of social media may be subject to disciplinary action. Disciplinary actions are subject to applicable policy or collective bargaining agreement.

Employee Name: _____

Employee Signature: _____

Date_____

Department Head/Elected Official Name: _____

Department Head/Elected Official Signature: _____

Date_____

Attachment 3
PHOTOGRAPHY CONSENT FORM / RELEASE

I, (print name)_____, hereby grant permission to Tillamook County representatives, to take and use: photographs and/or digital images of me for use in news releases and/or advertising. These materials might include printed or electronic publications, Web sites or other electronic communications. I further agree that my name and identity may be revealed in descriptive text or commentary in connection with the image(s). I authorize the use of these images without compensation to me. All negatives, prints, digital reproductions shall be the property of Tillamook County.

_____
(Date)

_____
(Signature of adult subject)

_____
(Address)

_____
(City, State, Zip)

RELEASE FOR MINOR CHILDREN (Under 18)

I, (print name) _____, parent or official guardian of (child's name)_____hereby grant permission to Tillamook County representatives, to take and use: photographs and/or digital images of **my child** for use in news releases and/or advertising materials as follows: printed publications or materials, electronic publications, or Web sites. I agree that my child's name and identity: may be revealed in descriptive text or commentary in connection with the image(s). I authorize the use of these images without compensation to me. All negatives, prints, digital reproductions and shall be the property of Tillamook County.

_____
(Date)

_____
(Signature of Parent or Guardian)

_____
(Address)

_____
(City, State, Zip)

ADMINISTRATIVE POLICY

SECTION: Information Services	Policy: IS-5	
TITLE: Remote Access	ORDER #: 21-057	
DEPT: Information Services		
ADOPTED: 10/27/2021	REVIEWED: TBD	REVISED: TBD

1. **PURPOSE/OBJECTIVE:**

1.1 The purpose of this policy is to authorize the Tillamook County Information Services (IS) Department to develop, implement, utilize, and improve security and associated processes and procedures needed to enable remote access to county IS resources.

2. **APPLICABILITY:**

2.1 All county departments, officials, employees, contractors, business partners, and volunteers

3. **VIOLATIONS:**

3.1 County officials, county employees, contractors, consultants, temporary staff, and/or volunteers who engage in improper use of information technology and electronic communications under this policy are subject to disciplinary action, up to and including dismissal.

4. **GENERAL POLICY:**

4.1 The purpose of this policy is to authorize the Tillamook County IS Department to develop, implement, utilize, and improve security and associated processes and procedures needed to enable remote access to county IS resources.

4.2 This policy aligns with Tillamook County, General Administration Telework Policy, GA-3.

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

5. **POLICY GUIDLINES:**

5.1 RESPONSIBILITIES

5.1.1 County IS resources may only be accessed remotely through capabilities implemented and maintained by the Tillamook County IS Department.

5.1.2 It is the responsibility of the IS Department to develop, own, and maintain processes and procedures defining creation, implementation, and ongoing support of remote access.

5.1.3 It is recognized that some county IT resources may not be viable candidates for remote access due to technical constraints, security limitations, or agreed-upon business practices.

5.1.3.1 A list of services for which remote access is available is maintained on the IS Department intranet page http://intranet.co.tillamook.or.us/V3/Default.htm

5.1.4 A completed and signed remote access request form is required prior to issuance of a remote access account and password.

5.1.5 Each department head is responsible for:

5.1.5.1 Determining departmental use of supported remote access capabilities and determining the person(s) to whom remote access may be made available based on departmental business needs.

5.1.5.2 Requesting remote access for authorized users via the IS Department Remote Access Request Process; and

5.1.5.3 Ensuring that the use of remote access complies with personnel rules and collective bargaining agreements.

5.1.6 Use of remote access shall comply with all county policies.

5.1.7 Remote access accounts and passwords may be used with:

5.1.7.1 County-owned equipment.

5.1.7.2 Approved Personal equipment, such as mobile devices, used to perform limited county business functions as approved by the authorizing department head or elected official and IS Department; or

5.1.7.3 Vendor-owned equipment for external parties having approval to connect to county owned equipment as outlined in 8.1.9 and 8.1.10, below.

5.1.8 Remote access may be requested for employees, volunteers, and external approved business partners on a one-time, intermittent, or ongoing basis depending upon business need.

5.1.8.1 Duration of access should be requested only for the time needed to conduct county business remotely.

5.1.8.2 To extend the remote access duration, a new request must be submitted.

5.1.9 Remote access for external business partners typically occurs as a scheduled event under supervision of IS staff.

5.1.9.1 An example of scheduled remote access is a collaborative work session between staff and a vendor representative for installation or upgrade of an application or other system resource.

5.1.10 Ongoing and unsupervised remote access may be established under special circumstances to allow connection by authorized external parties to county-owned IT resources for completion of specific contractually defined tasks supporting Tillamook County's operating environment when scheduled remote access would delay delivery of services. For example, an after-hours triage and troubleshooting for vendors required to provide 24x7 services.

5.1.11 Activities performed via remote access shall comply with county policies, state ethics and elections laws, administrative rules, federal, state, and local law, as well as any signed contractual agreements with external parties. When working remotely, employees are responsible to maintain restricted and confidential access to County electronic communications and equipment as confidential and only to approved County personnel. Employees are prohibited from giving access to County electronic communication devices or information to non-County employees or persons not specifically authorized to use or view County communication devices. Failure to adhere to these standards may be grounds for disciplinary action.

5.1.12 Data created or maintained via remote access is subject to State of Oregon public records laws and retention schedules. Any data created and stored while accessing county IT resources via remote access is a public record.

5.1.13 Data created or maintained via remote access shall comply with county policies to ensure the confidentiality, integrity, and availability of the data.