AGENDA ITEM FOR ADMINISTRATIVE MEETING ( ) Discussion only
(X) Action

FROM (DEPT/ DIVISION): Dan Lonai, Administrative Services

PROGRAM: IT

SUBJECT: Cybersecurity Policy

Administrative Services is requesting the approval and the adoption of the attached Cybersecurity Policy. This policy is required before the county can qualify for a higher tiered cyber insurance through our property and liability insurance carrier	ACTION REQUESTED: Adopt the Cybersecurity policy, Policy No. AS-14.0

ATTACHMENTS: Proposed Policy

Date:12/11/2023 Submitted By: (Dan Lonai)

**********For Internal Use Only**********

Checkoffs:
( ) Dept. Head (copy)
( ) Human Resources (copy)
( ) Budget (copy)
( ) Fiscal
( ) Legal (copy)
( ) (Other - List:

To be notified of Meeting:
Dan Lonai & Riley Wortman

Needed at Meeting:
)

****

Scheduled for meeting on: December 20, 2023

Action taken:

****

Follow-up:

Umatilla County

Cybersecurity Policy
AS-14.0

Table of Contents

Objective

The focus of this policy is to help Umatilla County meet its objectives. We recognize that information and the protection of information is required to serve our citizens. We seek to to ensure that appropriate measures are implemented to protect our citizen's information. This Cybersecurity Policy is designed to establish a foundation for an organizational culture of security. This policy will be reviewed annually by Administrative Services Director and approved by the Board of Commissioners

The purpose of this policy is to clearly communicate the Umatilla County security objectives and guidelines to minimize the risk of internal and external threats while taking advantage of opportunities that promote our objectives.

This policy applies to all Umatilla County elected officials, employees, contractors, consultants, volunteers and others specifically authorized to access information and associated assets owned, operated, controlled, or managed by Umatilla County. Additionally, leadership must ensure that all contracts and similar agreements with business partners and service providers incorporate appropriate elements of this policy.

Compliance

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

Roles and Responsibilities

Umatilla County has appointed the following roles and responsibilities to execute and monitor the policies described in this document.

Director of Administrative Services

- Ensure that a written Cybersecurity Policy is developed and implemented.
- Confirm identification, acquisition, and implementation of information system software and hardware.

IT Program Manager

- Identify all Personally Identifiable Information.
- Ensure implementation, enforcement, and effectiveness of IT Security policies and procedures.
- Facilitate an understanding and awareness that security requires participation and support at all organizational levels.
- Oversee daily activities and use of information systems to ensure employees, business partners, and contractors adhere to these policies and procedures.

Employees and Contractors

- See Appendix A - Acceptable Use Policy

Identify, Protect, Detect, Respond, and Recover

The following sections outline Umatilla County 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***.

The scope of security controls addressed in this policy focus on the activities most relevant to Umatilla 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 Director of Administrative Services or the IT Program Manager.

IDENTIFY (ID)

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

Asset Management

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

- The employee in possession of the hardware or software.
- Date of purchase.
- Amount of purchase.
- Serial number.
- Type of device and description.

Personally Identifiable Information (PII)

An inventory of all PII information by type and location will be taken. This inventory will be managed and reviewed by the Umatilla County IT Department.

Each department 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 your entity's record retention plan that outlines what information must be kept, and dispose of it securely once it is no longer required to maintain.

All PII no longer needed shall be shredded if in paper form or destroyed by the Umatilla County IT Department if in electronic form.

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

- Printing a consumer's SSN on any mailed materials not requested by the consumer unless redacted
- Printing a consumer's SSN on a card used by the consumer that is required to access products or services
- Publicly posting or displaying a consumer's SSN, such as on a website

Exceptions include requirements by state or federal laws, including statute 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.

PROTECT (PR)

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

Identity Management, Authentication and Access Control

The Director of Administrative Services is responsible for ensuring that access to the organization's systems and data is appropriately controlled. All systems housing Umatilla County data (including laptops, desktops, tablets, and cell phones) are required to be protected by two factor authentication wherever possible. If two factor authentication is not possible, the data should be protected with a password that conforms with the requirements below. . Except for the instances noted in this policy, users with access to Umatilla County systems and data are not to share passwords with anyone.

Password Requirements
For information on the Umatilla County Password Requirements see A.S. 5.0.

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

- Users are granted access only to the system data and functionality necessary for their job responsibilities.
- 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.
- All user access requests must be approved by the Umatilla County IT Department.
- It is the responsibility of the Umatilla County IT Department. to ensure that all employees and contractors who separate from the organization have all system access removed immediately.

On an annual basis, a review of user access will be conducted under the direction of IT Program Manager to confirm compliance with the access control policies outlined above.

Awareness and Training

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

1. All new hires are required to complete security awareness training to receive login credentials.
2. Formal security awareness refresher training is conducted on no less than an annual basis. All employees are required to participate in and complete this training.
3. A user will be required to complete additional security awareness training after a failed phishing exercise.

Upon completion of training, participants will review and sign the ***Acceptable Use Policy*** included in Appendix A.

On a monthly basis, Umatilla 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.

Data Security

Data Classification

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

- **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.
- **Operational**: Includes data for basic organizational operations, communications with vendors, employees, etc. (non-confidential). This includes any data that is available or requestable by the general public. The majority of data will fall into this category.
- **Confidential:** Any information deemed confidential. The following list provides guidelines on what type of information is typically considered confidential. Confidential data may include:
    - Employee or customer Social Security numbers or personally identifiable information (PII)
    - Personnel files
    - Medical and healthcare information
    - Protected Health Information (PHI)
    - Network diagrams and security configurations
    - Communications regarding legal matters
    - Passwords/passphrases
    - Bank account information and routing numbers
    - Payroll information
    - Credit card information
    - Any confidential data held for a third party (be sure to adhere to any confidential data agreement covering such information)

Data Storage

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

- **Operational:** Operational data should be stored on a server that gets the most frequent backups. Some type of system- or disk-level redundancy is encouraged.
- **Confidential**: Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored behind a locked door and in a locked computer or cabinet.

Data Transmission

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

- **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.

Data Destruction

You must follow your records retention policy before destroying data.

- **Confidential:** Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:
    - Paper/documents: Cross-cut shredding is required.
    - Storage media (CD's, DVD's): Physical destruction is required.
    - Hard drives/systems/mobile storage media: All Hard drives/systems/mobile storage media be cleared in accordance with the description in AS-4.0.

Data Storage

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

- Whole disk encryption
- Encryption of partitions/files
- Encryption of disk drives
- Encryption of personal storage media/USB drives
- Encryption of backups
- Encryption of data generated by applications

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

- VPN tunnels
- Remote access sessions
- Web applications
- Email and email attachments
- Remote desktop access
- Communications with applications/databases

Information Protection Processes and Procedures

Secure Software Development

Where applicable, all software development activities performed by Umatilla County or by vendors on behalf of the organization shall employ secure coding practices including those outlined below.

A minimum of three software environments for the development of software systems should be available – development, quality assurance, and a production environment. Software developers or programmers are required to develop in the development environment and promote objects into the quality assurance and production environments. The quality assurance 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 IT Program Manager or an independent peer review will be required for promotion of objects into the production environment.

- All production changes must be approved before being promoted to production.
- All production changes must be developed in the development environment and tested in the quality assurance environment.
- All emergency changes must be adequately documented and approved.

Software code approved for promotion will be uploaded by the Umatilla County IT Department to the production environment from the quality assurance environment once the change request is approved. The Umatilla County IT Department may work with the developer to ensure proper placement of objects into production.

Contingency Planning

The organization's business contingency capability is based upon local and cloud backups of all critical business data. This critical data is defined as data containing PII, operational, or confidential data. Full data backups will be performed on at least a monthly basis. Confirmation that backups were performed successfully will be conducted bi-weekly. Testing of local and cloud backups as well as their restoration capability will be performed on a biannual basis.

During a contingency event, all IT decisions and activities will be coordinated through and under the direction of the Director of Administrative Services or the IT Program Manager.

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

- In the event that one or more of Umatilla County 's systems or applications are deemed corrupted or inaccessible, the Director of Administrative Services or the IT Program Manager will work with the respective individuals/vendor(s) to restore data from the most recent cloud or local backup and, if necessary, acquire replacement hardware.

- In the event that the location housing the Umatilla County systems are no longer accessible, the Director of Administrative Services or the IT Program Manager 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.

Network Infrastructure

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

- Vendor recommended, and industry standard configurations will be used.
- Changes to firewall and router configuration will be approved by the Director of Administrative Services or the IT Program Manager.
- Both router and firewall passwords must be secured and difficult to guess.
- The default policy for the firewall for handling inbound traffic should be to block all packets and connections unless the traffic type and connections have been specifically permitted.
- Inbound traffic containing ICMP (Internet Control Message Protocol) traffic should not be passed in from the Internet, or from any un-trusted external network.
- All web services running on routers must be disabled.
- Simple Network Management Protocol (SNMP) Community Strings must be changed from the default "public" and "private".

Network Servers

Servers typically accept connections from several sources, both internal and external. As a general 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:

- 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.
- Network servers, even those meant to accept public connections, must be protected by a firewall or access control list.
- If possible, a standard installation process should be developed for the organization's network servers. A standard process will provide consistency across servers no matter what employee or contractor handles the installation.

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

Network Segmentation

Network segmentation is used to limit access to data within the Umatilla County network based upon data sensitivity.
All wireless networks are to be physically separated to prevent access to internal secure networks.

Additional network segmentation should be implemented to limit risk to other segments of the internal network if one segment of the network is compromised. Network segments should be based upon data sensitivity and security requirements set forth by the Director of Administrative Services or the IT Program Manager.
Under the direction of the Director of Administrative Services or the IT Program Manager, the network administrator manages the network user accounts, monitors firewall logs, and operating system event logs. The Umatilla County IT Department authorizes vendor access to the system components as required for maintenance.

Protective Technology

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. Umatilla 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.

Additionally, software solutions 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 Director of Administrative Services or the IT Program Manager.

Network Vulnerability Assessments

On at least a monthly basis, Umatilla 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 the Director of Administrative Services or the IT Program Manager to identify weaknesses with the network configuration that could allow unauthorized and/or unsuspected access to the organization’s data and systems.

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)

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

Anomalies and Events

The following logging activities are conducted by IT:

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

Passwords should not be contained in logs.

Logs of the above events will be reviewed by IT at least once per month. Event logs will be configured to maintain record of the above events for three months.

Security Continuous Monitoring

Anti-Malware Tools

All organization servers and workstations will utilize an endpoint agent 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 any results from the endpoint agent dashboard will be conducted by the Director of Administrative Services or the IT Program Manager to confirm the status of virus definition updates and scans.

Umatilla County utilizes an MDM system to protect mobile devices from malware and viruses.

Patch management

All software updates and patches will be distributed to all Umatilla County system as follows:

- Workstations will be configured to install software updates every week automatically.
- Server software updates will be manually installed at least monthly.
- Any exceptions shall be documented.

RESPOND (RS)

Definition: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

Response Planning

The organization's annual security awareness 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 Umatilla County 's information assets, can be defined as either an Electronic or Physical Incident.

The Director of Administrative Services or the IT Program Manager 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.

Electronic Incidents

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.

1. Remove the compromised device from the network by unplugging or disabling network connection. Do not power down the machine.
2. Report the incident to the Director of Administrative Services or the IT Program Manager.
3. Contact the third-party service provider (and/or computer forensic specialist) as needed.

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

4. Disable the compromised account(s) as appropriate.
5. Certify that the network the computer was connected to is clean.
6. Backup all data and logs on the machine, or copy/image the machine to another system.
7. Determine exactly what happened and the scope of the incident.
8. Determine how the attacker gained access and disable it.
9. Rebuild the system, including a complete operating system reinstall.
10. Restore any needed data from the last known good backup and put the system back online.
11. Take actions, as possible, to ensure that the vulnerability will not reappear.

12. Conduct a post-incident evaluation. What can be learned? What could be done differently?

Physical Incidents

A physical IT 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 Director of Administrative Services or the IT Program Manager.

Notification

If an electronic or physical security incident is suspected of having resulted in the loss of third-party/customer data, notification of the public or affected entities should occur.

1. Contact CIS Claims at claims@cisoregon.org.
2. County's liability insurance Agent of Record.
3. Inform your attorney
4. Board of Commissioners
5. Complete this form if the breach involves more than 250 records. https://justice.oregon.gov/consumer/DataBreach/Home/Submit

RECOVER (RC)

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

CIS will help with the recovery process. CIS may provide forensics services, breach coaching services, legal services, media services and assist in paying for notification expenses. The CIS claims adjuster will discuss with you the coverages and services offered by CIS.

The Director of Administrative Services or the IT Program Manager is responsible for managing and directing activities during an incident, including the recovery steps.

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

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

External communications should only be handled by designated individuals at the direction of the Director of Administrative Services or the IT Program Manager. Recovery activities are communicated to internal stakeholders, executives, and management teams.

Appendix A – Acceptable Use Policy

The intention of this Acceptable Use Policy is not to impose restrictions that are contrary to Umatilla County's established culture of openness, trustworthiness, and uprightness. Understanding and adhering the organization's IT security policies is necessary to protect our employees and organization from illegal or damaging actions by individuals, either knowingly or unknowingly. Effective security is a team effort involving the participation and support of every employee. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment, email, and internet access at all locations. These rules are in place to protect the employee and the organization. Inappropriate use exposes the organization to risks including virus attacks, compromises of network systems and services, and legal liability.

Scope

This policy applies to both permanent employees, temporary employees, elected officials, contractors, and volunteers of the organization. This policy applies to all equipment that is owned or leased by the organization. This policy is a supplement to the *Umatilla County Cybersecurity Policy*.

1.0 Policy

The following actions shall constitute unacceptable use of the corporate network. The list also provides a frame of reference for types of activities that are deemed unacceptable. The user may not use the corporate network and/or systems to:

1. Engage in an activity that is illegal under local, state, federal, or international law.
2. Engage in any activities that may cause embarrassment, loss of reputation, or other harm to the organization.
3. Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, threatening, obscene or otherwise inappropriate messages or media.
4. Engage in activities that cause an invasion of privacy.
5. Engage in activities that cause disruption to the workplace environment or create a hostile workplace based on a legally protected class.
6. Make fraudulent offers for products or services.
7. Install, download or distribute unlicensed or "pirated" software.
8. Reveal personal or network passwords to others, including family, friends, or other members of the household when working from home or remote locations.

Email

The following activities are strictly prohibited:

1. Using the email system to send or forward pornographic material.
2. Using the email system for any form of harassment whether through language, content, frequency or size of the message.
3. Sending unsolicited bulk email messages, including the sending of “junk mail” or other advertising materials to individuals who did not specifically request such material (email spam).
4. Sending or forwarding emails of a non-business nature to the “All Employee” list.
5. Sending or forwarding emails of a non-business nature with either an excessive number of attachments or attachments of excessive size (examples would be emails with numerous photos, video clips, or large PowerPoint presentations).
6. Creating or forwarding “chain letters,” “Ponzi” schemes or other get rich quick “pyramid” schemes of any type.
7. Using the email system in a manner that would violate the Umatilla County Cybersecurity Policy.
8. Opening file attachments with file extensions such as .vbs, .exe, .com, or .sys.

Social Networking/Blogging

The following applies to social networking/blogging:

1. Employees are discouraged from using employer-owned equipment, including computers, organizationally licensed software or other electronic equipment, or organization time to conduct personal blogging. Social networking activities are discouraged.
2. Employees are expected to protect the privacy of the organization and its employees and are prohibited from disclosing personal employee and nonemployee information and any other proprietary and nonpublic information to which the employees have access.
3. Management strongly urges employees to report any violations or possible violations or perceived violations to supervisors or managers. Management investigates and responds to all reports of violations of the social networking policy and other related policies.
4. Only executive management are authorized to remove any content that does not meet the rules and guidelines of the policy or that may be illegal or offensive.
5. Views of the individual employee are not ever attributed to Umatilla County.
6. Posts must comply with existing policies re: harassment and discrimination.
7. Posts must comply with existing policies re: confidentiality and improper disclosures.
8. Online activities must not interfere or negatively affect work tasks or Umatilla County, except for “Concerted Activities.”

9. Employees must not reference Umatilla County or its services in the employee's social medial posts, except for "Concerted Activities."
10. Umatilla County logos should not be used in the employee's social media posts, except for "Concerted Activities."
11. Posts must not violate copyright laws.
12. Consult Umatilla County Policies and Procedures for further clarification.

Clean Desk

A significant amount of confidential customer information is maintained in paper-based form. All staff members are responsible for ensuring that this information is properly safeguarded and is not improperly disclosed to unapproved third parties. In order to accomplish this, all employees are responsible for:

1. Ensuring that paper-based information is appropriately monitored and protected.
2. Ensuring that all confidential documents are properly locked-up at the end of each business day. Appropriate methods to secure documents include utilizing locking filing cabinets or desk drawers, etc.
3. Maintaining a "clean desk" or working area throughout the day and ensuring there are no confidential documents in open view if absent from their desk for an extended period. This will help to ensure that confidential customer information is not inadvertently disclosed.

Computer Usage (Password)
For information on the Umatilla County Password Requirements see Appendix C - Password Policy or A.S. 5.0.

Portable Devices

The following Umatilla County Portable Devices are allowed for organization use only:

1. Cell phones
2. Laptops
3. Tablets
4. Digital cameras
5. Any type of USB memory device or USB mass storage device

2.0 Monitoring

Employees should have no expectation of privacy for any information they store, send, receive, or access via the organization's network. Content monitoring of email by management may occur without prior notice. All other monitoring, including but not limited to, internet activity, email

volume or size, and other forms of electronic data exchange may occur without prior notice by management.

Monitoring may occur without prior notice of a suspected violation, either in part or in whole, of the Acceptable Use Policy or the *Umatilla County Cybersecurity Policy* is detected or reported.

3.0 Reporting

Employees must report to the Umatilla County IT Department when they learn of a suspected breach of information or have lost a laptop, telephone, or USB memory with Umatilla County information.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Signature

I have received a copy of the organization's Acceptable Use Policy as revised and approved by the management. I have read and understood the policy.

_____
(Print your name)

_____ _____
(Signature) (Date)