

[City/County/Entity]

## **Cybersecurity Policy**

## Table of Contents

Roles and Responsibilities .....	3
IDENTIFY (ID) .....	4
Asset Management .....	4
PROTECT (PR) .....	5
Identity Management, Authentication and Access Control .....	5
Awareness and Training .....	6
Data Security .....	7
Data Classification .....	7
Data Storage .....	7
Data Transmission .....	8
Data Destruction .....	8
Data Storage .....	8
Information Protection Processes and Procedures .....	9
Secure Software Development .....	9
Contingency Planning .....	9
Network Infrastructure .....	10
Network Servers .....	10
Protective Technology .....	11
Email Filtering .....	11
Network Vulnerability Assessments .....	11
DETECT (DE) .....	12
Anomalies and Events .....	12
Security Continuous Monitoring .....	12
Anti-Malware Tools .....	12
Patch management .....	12
RESPOND (RS) .....	13
Response Planning .....	13
Electronic Incidents .....	13
Physical Incidents .....	14
Notification .....	14
RECOVER (RC) .....	14
Appendix A – Acceptable Use Policy .....	15
Appendix B – Confidentiality and Non-Disclosure Agreement .....	19

## Objective

The focus of this policy is to help [City/County/Entity] meet its objectives. We recognize 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 citizen's information. This Cybersecurity Policy is designed to establish a foundation for an organizational culture of security. This policy will be reviewed annually and approved by the [TITLE].

The purpose of this policy is to clearly communicate the [City/County/Entity] 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 [City/County/Entity] elected officials, employees, contractors, consultants, and others specifically authorized to access information and associated assets owned, operated, controlled, or managed by [City/County/Entity]. 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.

<https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/data-breaches/>

## ***Roles and Responsibilities***

[City/County/Entity] has appointed the following roles and responsibilities to execute and monitor the policies described in this document.

[TITLE]

- Ensure that a written Cybersecurity Policy is developed and implemented.
- Confirm identification, acquisition, and implementation of information system software and hardware.
- 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 [City/County/Entity] 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 [City/County/Entity] 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 [TITLE].

**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 [City/County/Entity] 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.
- A listing of software or devices that have been restricted.

**Personally Identifiable Information (PII)**

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

Location	PII by type	Essential	Location	Owner
Website				
Contractors				
File in staff office				
File in building				

File offsite				
Desk top				
HR System				
Financial System				
Laptop				
Flash drive				
Cell phones				
Tablets				
Other				

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 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 IT 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***

[TITLE] is responsible for ensuring that access to the organization’s systems and data is appropriately controlled. All systems housing [City/County/Entity] 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 [City/County/Entity] systems and data are not to share passwords with anyone.

[City/County/Entity] has established following password configuration requirements for all systems and applications (where applicable):

- Minimum password length: 8 characters
- Password complexity: requires alphanumeric and special characters
- Prohibited reuse for four (4) iterations
- Changed periodically every 90 days
- Invalid login attempts set to three
- Automatic logout due to inactivity = 30 minutes

Other potential safeguards include:

- Not allowing PII on mobile storage media
- Locking file cabinets
- Not allowing PII left on desktops
- Encrypting sensitive files on computers
- Requiring password protection
- Implementing the record retention plan and destroying records no longer required

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 [TITLE].
- It is the responsibility of [TITLE] to ensure that all employees and contractors who separate from the organization have all system access removed within [TIMEFRAME].

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

### ***Awareness and Training***

[City/County/Entity] personnel are required to participate in security training in the following instances:

1. All new hires are required to complete security awareness training before receiving login credentials.
2. Formal security awareness refresher training is conducted on an annual basis. All employees are required to participate in and complete this training.

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

Two online classes are available through the CIS Learning Center at [learn.cisoregon.org](http://learn.cisoregon.org): “*Cyber Threats and Best Practices to Confront Them*” and “*Cyber Security Basics*.”

On an annual basis, [City/County/Entity] 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.
- **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.
- **Operational:** Includes data for basic organizational operations, communications with vendors, employees, etc. (non-confidential). 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 (refer to the Backup Policy for additional information). 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 under lock and key (or keycard/keypad), with the key, keycard or code secured.

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

#### 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 [City/County/Entity] 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 information technology manager or an independent peer review will be required for promotion objects into the production environment.

- All production changes must be approved before being promoted to production.
- Developers should not have the ability to move their own code.
- All production changes must have a corresponding help desk change request number.
- 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 [TITLE] to the production environment from the quality assurance environment once the change request is approved. The [TITLE] may work with the developer to ensure proper placement of objects into production.

### Contingency Planning

The organization's business contingency capability is based upon [CLOUD or LOCAL] backups of all critical business data. This critical data is defined as [CRITICAL DATA DEFINITION]. Full data backups will be performed on a [FREQUENCY] basis. Confirmation that backups were performed successfully will be conducted [FREQUENCY]. Testing of cloud backups and restoration capability will be performed on a [FREQUENCY] basis.

During a contingency event, all IT decisions and activities will be coordinated through and under the direction of the [TITLE].

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

- In the event that one or more of [City/County/Entity] 's systems or applications are deemed corrupted or inaccessible, the [TITLE] will work with the respective 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 [City/County/Entity] systems are no longer accessible, the [TITLE] 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.

*As an important reminder, CIS covers data reproduction (subject to a deductible) for only one week.*

### 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 [TITLE].
- 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 [City/County/Entity] network based upon data sensitivity. [City/County/Entity] maintains two wireless networks. The *guest* wireless network is password protected, and proper authentication will grant the user internet access only. Access to the *secure* wireless network is limited to [ORGANIZATION] personnel and provides the user access to the intranet.

*The following paragraph can be included if a third-party vendor is used for network administration:*

Under the direction of the [TITLE], the third-party network administrator manages the network user accounts, monitors firewall logs, and operating system event logs. The [TITLE] authorizes vendor access to the system components as required for maintenance.

#### **Additional Considerations**

Does the organization employ industry-accepted configurations/standards for mobile devices, laptops, workstations, and other hardware and software?

### ***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. [City/County/Entity] 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, [EMAIL OR ANTI-MALWARE PROGRAMS] 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 IT Manager.

#### Network Vulnerability Assessments

On a [FREQUENCY] basis, [City/County/Entity] 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 [TITLE] 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.

**Additional Considerations**

Does the organization have technologies (e.g., web proxies/web filtering) in place that limit a user's access to dangerous or malicious sites?

Does the organization monitor the flow of data across the network?

Does the organization employ web application firewalls on web servers, if you host your own website?

**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 [POSITION] under the direction of [TITLE]:

- 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 the [POSITION] 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 [TOOL] 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 [TOOL] dashboard will be conducted by [TITLE] to confirm the status of virus definition updates and scans.

[City/County/Entity] utilizes [TOOL] to protect mobile devices from malware and viruses.

Patch management

All software updates and patches will be distributed to all [City/County/Entity] 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.

**Additional Considerations**

Does the organization manage the ongoing use of ports, protocols, and services on networked devices to minimize vulnerabilities?

**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 [City/County/Entity]'s information assets, can be defined as either an Electronic or Physical Incident.

[TITLE] 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 [TTLE] or [TITLE].
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. Backup all data and logs on the machine, or copy/image the machine to another system.
6. Determine exactly what happened and the scope of the incident.
7. Determine how the attacker gained access and disable it.
8. Rebuild the system, including a complete operating system reinstall.
9. Restore any needed data from the last known good backup and put the system back online.

10. Take actions, as possible, to ensure that the vulnerability will not reappear.
11. 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 [TTLE] or [TITLE].

### 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](mailto:claims@cisoregon.org).
2. Inform your attorney
3. 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.

[TITLE] 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 [TITLE]. 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 [City/County/Entity] 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 and temporary employees of the organization. This policy applies to all equipment that is owned or leased by the organization. This policy is a supplement to the [City/County/Entity] *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 [City/County/Entity] 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 for 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 the [City/County/Entity] .
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 [City/County/Entity], except for “Concerted Activities.”
9. Employees must not reference [City/County/Entity] or its services in the employee’s social medial posts, except for “Concerted Activities.”
10. [City/County/Entity] 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 the Employee Personnel Handbook 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 ensure 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)*

The following password criteria will be used to access Windows workstations:

1. Minimum password length: 8 characters
2. Password complexity: requires alphanumeric and special characters
3. Prohibited reuse for four (4) iterations
4. Changed periodically every 90 days
5. Invalid login attempts set to three
6. Automatic logout due to inactivity = 30 minutes

### *Portable Devices*

The following Portable Devices are allowed for organization use only:

1. Cell phones
2. Laptops
3. Digital cameras
4. 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 [City/County/Entity] *Cybersecurity Policy* is detected or reported.

**3.0 Reporting**

Employees must report to [TITLE] when they learn of a suspected breach of information or have lost a laptop, telephone, or USB memory with [City/County/Entity] 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)

## Appendix B – Confidentiality and Non-Disclosure Agreement

This Confidentiality and Nondisclosure Agreement (the "Agreement") is entered into by and between [City/County/Entity] ("Disclosing Party") and \_\_\_\_\_ ("Receiving Party") for the purpose of preventing the unauthorized disclosure of Confidential Information as defined below. The parties agree to enter into a confidential relationship with respect to the disclosure of certain proprietary and confidential information ("Confidential Information").

1. Definition of Confidential Information. For purposes of this Agreement, "Confidential Information" shall include all information or material that has or could have commercial value or other utility in the business in which Disclosing Party is engaged. Examples of Confidential Information include the following:
  - Employee or customer Social Security numbers or personal information
  - Customer data
  - Entity financial data
  - Product and/or service plans, details, and schematics,
  - Network diagrams and security configurations
  - Communications about entity legal matters
  - Passwords
  - Bank account information and routing numbers
  - Payroll information
  - Credit card information
  - Any confidential data held for a third party
2. Exclusions from Confidential Information. Receiving Party's obligations under this Agreement do not extend to information that is: (a) publicly known at the time of disclosure or subsequently becomes publicly known through no fault of the Receiving Party; (b) discovered or created by the Receiving Party before disclosure by Disclosing Party; (c) learned by the Receiving Party through legitimate means other than from the Disclosing Party or Disclosing Party's representatives; or (d) is disclosed by Receiving Party with Disclosing Party's prior written approval.
3. Obligations of Receiving Party. Receiving Party shall hold and maintain the Confidential Information in strictest confidence for the sole and exclusive benefit of the Disclosing Party. Receiving Party shall carefully restrict access to Confidential Information to employees, contractors, and third parties as is reasonably required and shall require those persons to sign nondisclosure restrictions that are at least as protective as those in this Agreement. Receiving Party shall not, without the prior written approval of Disclosing Party, use for Receiving Party's own benefit, publish, copy, or otherwise disclose to others, or permit the use by others for their benefit or to the detriment of Disclosing Party, any Confidential Information. Receiving Party shall return to Disclosing Party any and all records, notes, and other written, printed, or tangible materials in its possession pertaining to Confidential Information immediately if Disclosing Party requests it in writing.
4. Time Periods. The nondisclosure provisions of this Agreement shall survive the termination of this Agreement and Receiving Party's duty to hold Confidential Information in confidence

shall remain in effect until the Confidential Information no longer qualifies as a trade secret or until Disclosing Party sends Receiving Party written notice releasing Receiving Party from this Agreement, whichever occurs first.

5. Relationships. Nothing contained in this Agreement shall be deemed to constitute either party a partner, joint venturer or employee of the other party for any purpose.
6. Severability. If a court finds any provision of this Agreement invalid or unenforceable, the remainder of this Agreement shall be interpreted so as best to affect the intent of the parties.
7. Integration. This Agreement expresses the complete understanding of the parties with respect to the subject matter and supersedes all prior proposals, agreements, representations, and understandings. This Agreement may not be amended except in a writing signed by both parties.
8. Waiver. The failure to exercise any right provided in this Agreement shall not be a waiver of prior or subsequent rights.

This Agreement and each party's obligations shall be binding on the representatives, assigns, and successors of such party. Each party has signed this Agreement through its authorized representative.

**Disclosing Party**

By: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Title: \_\_\_\_\_

Dated: \_\_\_\_\_

**Receiving Party**

By: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Title: \_\_\_\_\_

Dated: \_\_\_\_\_