

RESOLUTION NO. 21-03

A RESOLUTION IMPLEMENTING WRITTEN POLICIES AND PROCEDURES FOR CYBERSECURITY PROTECTION.

WHEREAS, The City of Irrigon uses data and networking technology systems in its operations;

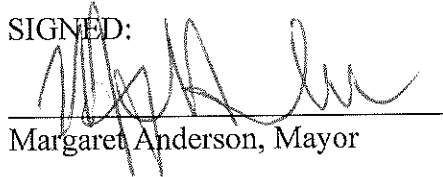
WHEREAS, there is a need to protect such systems; and

WHEREAS, ORS 646A.622 (d) requires an entity to implements an information security program that includes administrative safeguards, technical safeguards and physical safeguards;

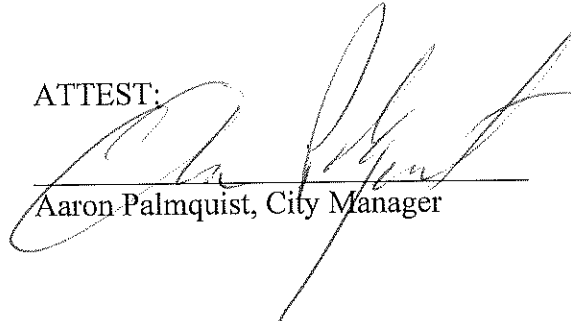
NOW, THEREFORE BE IT HEREBY RESOLVED BY THE COMMON COUNCIL OF THE CITY OF IRRIGON THAT THE ATTACHED CYBERSECURITY POLICY FOR THE CITY OF IRRIGON IS ADOPTED:

ADOPTED BY THE COMMON COUNCIL AND EFFECTIVE ON THE 16th DAY OF March 2021.

SIGNED:


Margaret Anderson, Mayor

ATTEST:


Aaron Palmquist, City Manager

City of Irrigon

Cybersecurity Policy

(3/16/2021)

Table of Contents

Roles and Responsibilities	3
IDENTIFY	4
Asset Management.....	4
PROTECT	5
Identity Management, Authentication and Access Control.....	5
Awareness and Training	6
Data Security	6
Data Classification.....	6
Data Storage	7
Data Transmission	7
Data Destruction.....	7
Data Storage	8
Information Protection Processes and Procedures.....	8
Contingency Planning	8
Network Infrastructure	9
Network Servers.....	9
Protective Technology	10
Email Filtering.....	10
Network Vulnerability Assessments	10
DETECT	10
Anomalies and Events	10
Security Continuous Monitoring	11
Anti-Malware Tools.....	11
Patch management	11
RESPOND	11
Response Planning	11
Electronic Incidents	12
Physical Incidents.....	12
Notification.....	12
RECOVER	12
Appendix A – Acceptable Use Policy	14
Appendix B – Confidentiality and Non-Disclosure Agreement.....	18

Objective

The focus of this policy is to help City of Irrigon meet its objectives. We recognize that information and the protection of information is required to serve the public. We seek to ensure that appropriate measures are implemented to protect our customers' information. This Cybersecurity Policy is designed to establish a foundation for an organizational culture of security.

The purpose of this policy is to clearly communicate the City of Irrigon 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 of Irrigon elected officials, commissions, boards, employees, contractors, consultants, and others specifically authorized to access information and associated assets owned, operated, controlled, or managed by City of Irrigon. 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 of Irrigon has appointed the following roles and responsibilities to execute and monitor the policies described in this document.

City Manager

- 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 of Irrigon 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 of Irrigon 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 city manager.

IDENTIFY

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 of Irrigon 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 personally identifiable information by type and location will be taken.

Each manager or department head will determine if personally identifiable information is essential. If personally identifiable information 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 personally identifiable information 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

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

Identity Management, Authentication and Access Control

City manager is responsible for ensuring that access to the organization's systems and data is appropriately controlled. All systems housing City of Irrigon 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 of Irrigon systems and data are not to share passwords with anyone.

City of Irrigon has established following password configuration requirements for all systems and applications (where applicable):

- Minimum password length: 12 characters
- Password complexity: requires alphanumeric characters and special characters
- Prohibited reuse for four (4) iterations
- Changed periodically
- Invalid login attempts set to three
- Automatic logout due to inactivity = 30 minutes

Other potential safeguards include:

- Not allowing Personally Identifiable Information on mobile storage media
- Locking file cabinets
- Not allowing Personally Identifiable Information left on desktops
- Encrypting sensitive files on computers
- Requiring password protection

- Implementing the record retention plan and destroying records that are 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 their supervisor.
- It is the responsibility of city manager to ensure that all employees and contractors who separate from the organization have all system access removed within 24 hours.

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

Awareness and Training

City of Irrigon 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: "*Cyber Threats and Best Practices to Confront Them*" and "*Cyber Security Basics*."

On an annual basis, City of Irrigon may 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:

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.

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.
3. **Operational:** Includes data for basic organizational operations, communications with vendors, employees, etc. (non-confidential). The majority of data will fall into this category.
4. **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.

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.
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, with the key code secured.

Data Transmission

- **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

Contingency Planning

The organization's business contingency capability is based upon local backups of all critical business data. This critical data is defined as necessary data available to restore critical business functions as soon as possible after a disaster event. Full data backups will be performed on a weekly basis. Confirmation that backups were performed successfully will be conducted monthly. Testing of backups and restoration capability will be performed on a monthly basis.

During a contingency event, all IT decisions and activities will be coordinated through and under the direction of the city manager.

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

- In the event that one or more of City of Irrigon's systems or applications are deemed corrupted or inaccessible, the city manager will work with the respective vendor(s) to restore data from the most recent backup and, if necessary, acquire replacement hardware.
- In the event that the location housing the City of Irrigon systems are no longer accessible, the city 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 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 city manager.
- 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.
- 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 of Irrigon network based upon data sensitivity. City of Irrigon maintains one wireless network. Access to the *secure* wireless network is limited to City of Irrigon personnel and provides the user access to the internet.

Under the direction of the city manager, the third-party network administrator manages the network user accounts, monitors firewall logs, and operating system event logs. The city manager 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. City of Irrigon 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, anti-malware programs may be 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 an annual basis, City of Irrigon 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 city manager to identify weaknesses with the network configuration that could allow unauthorized and/or unsuspected access to the organization's data and systems.

DETECT

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 service providers under the direction of the city manager:

- 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 city manager 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 AVG Antivirus, Norton Antivirus or similar program 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 AVG Antivirus, Norton Antivirus or similar program dashboard will be conducted by city manager to confirm the status of virus definition updates and scans.

City of Irrigon utilizes AVG Antivirus, Norton Antivirus or similar program to protect mobile devices from malware and viruses.

Patch management

All software updates and patches will be distributed to all City of Irrigon system as follows:

- Workstations will be configured to install software updates automatically.
- Any exceptions shall be documented.

RESPOND

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 of Irrigon's information assets, can be defined as either an Electronic or Physical Incident.

City manager is responsible for coordinating all activities during a significant incident, including notification and communication activities. He/she 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 city 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. 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 city manager or direct supervisor.

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 for advice on how to proceed
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

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

As our insurance carrier, CIS may 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.

City 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 city 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 City of Irrigon established culture of openness, trustworthiness, and uprightness. Understanding and adhering to the organization's IT security policies is necessary to protect our employees, customers and city from illegal or damaging actions by individuals, either knowingly or unknowingly. Effective security is a team effort involving the participation and support of every elected official, employee, contractor and/or consultant. It is the responsibility of every computer or mobile device user to know these guidelines and to conduct their activities accordingly to safeguard information from unauthorized or inadvertent use, modification, disclosure or destruction.

Purpose

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

Scope

This policy applies to all elected officials, employees, contractors and/or consultants of the City of Irrigon. This policy applies to all equipment that is owned or leased by the organization. This policy is a supplement to the *City of Irrigon Cybersecurity Policy*.

1.0 Policy

The following actions shall constitute unacceptable use of the network. The list also provides a frame of reference for types of activities that are deemed unacceptable. The user may not use the 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 City of Irrigon, its employees, officials or associates.
3. Circulate 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.
9. Engage any personal financial gain or illegal activities

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. Creating or forwarding "chain letters," "Ponzi" schemes or other get rich quick "pyramid" schemes of any type.
6. Using the email system in a manner that would violate the City of Irrigon Cybersecurity Policy.
7. Opening file attachments with file extensions such as .vbs, .exe or .sys.
8. Opening any file attachments before utilizing virus checking procedures.
9. Any uses that could cause congestion, delay, degradation or disruption of service to any government system or equipment.

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 of Irrigon.
6. Posts must comply with existing policies regarding harassment and discrimination.
7. Posts must comply with existing policies regarding confidentiality and improper disclosures.
8. Online activities must not interfere or negatively affect work tasks for the City of Irrigon.
9. Employees must not reference City of Irrigon or its services in the employee's social media posts."
10. City of Irrigon logos should not be used in the employee's social media posts.
11. Posts must not violate copyright laws.

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

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

1. Minimum password length: 12 characters
2. Password complexity: requires alphanumeric characters and special characters
3. Prohibited reuse for four (4) iterations
4. Changed periodically
5. Invalid login attempts set to three
6. Automatic logout due to inactivity = 30 minutes

Use of computers for personal communications by e-mail and brief internet searches are permitted as long as they are before or after work hours, on break periods or lunch breaks and does not cause any adverse reflection on Irrigon; are of reasonable duration and does not violate City of Irrigon policies.

Portable Devices

All portable devices must have wireless capability disabled before connecting to the network. 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

Remote Access

Remote access will be conducted via terminal server access controller systems, virtual private network or outlook web access. City of Irrigon owned hardware and software will be used. The employee is the only individual authorized to use this equipment. Access will be as authorized by the supervisor.

Training

Users are required to participate in security training before accessing information systems of the City of Irrigon.

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 *City of Irrigon Cybersecurity Policy* is detected or reported.

3.0 Reporting

Employees must report to their immediate supervisor when they learn of any suspicious output, files, shortcuts, system problems or suspected breach of information or have lost a laptop, telephone, or USB memory with City of Irrigon information.

4.0 Enforcement

The ultimate responsibility for ensuring the protection of information lies with the user. The release of information is a security violation and will be investigated and handled accordingly.

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 of Irrigon** ("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
 - Client privilege information
 - Property items or code issues
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: _____