City of Hermiston, Oregon

Cybersecurity Policy

City Council Approval Copy, September 23, 2019

Table of Contents

Objective

The focus of this policy is for the City of Hermiston to meet its objective of optimal security for all of the city's computer/internet activities. 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 City Council.

The purpose of this policy is to clearly communicate the City of Hermiston security objectives and guidelines to minimize the risk of internal and external cyber threats.

This policy applies to all City of Hermiston elected officials, employees, contractors, consultants, and others specifically authorized to access information and associated assets owned, operated, controlled, or managed by the City of Hermiston.

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

The City of Hermiston has appointed the following roles and responsibilities to execute and monitor the policies described in this document.

Director of Finance

- 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 the City of Hermiston 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 the City of Hermiston 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 Finance.

IDENTIFY (ID)

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

Asset Management

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

- The department and location within that department of the hardware/software.
- Date of purchase of equipment and associated software.
- Amount of purchase(s).
- 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 conducted on an annual basis.

If this information does serve a need, the City of Hermiston will apply the appropriate 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

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

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

- Minimum password length: 15 characters
- Password complexity can be alphanumeric and special characters
- Prohibited reuse for four (3) iterations
- Changed periodically every 6 months (suggested)
- Invalid login attempts set to three
- Automatic logout due to inactivity = 10 minutes

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.
- All user access requests must be approved by the Director of Finance.
- It is the responsibility of the Director of Finance to ensure that all employees and contractors who separate from the organization have all system access removed within one (1) business day from date of separation.

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

Awareness and Training

City of Hermiston 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.

To facilitate the annual security training requirement, 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 a periodic basis, the City of Hermiston 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 the individual's 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

Adherence to the City of Hermiston's Records Retention Policy regarding the storage and destruction of data is required. Data residing on the City of Hermiston's 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. 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

All City of Hermiston personnel will follow the appropriate records required 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 Transmission

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 IMESD (Inter-Mountain Education Service District) backups of all critical business data. This critical data is defined as data that is critical to successfully carrying out the operations/daily functions of the City of Hermiston. Full data backups will be performed on a once-a-day basis. Confirmation that backups were performed successfully will be conducted daily. Testing of cloud backups and restoration capability will be performed on a quarterly basis.

During a contingency event, all IT decisions and activities will be coordinated through and under the direction of the City Manager and/or the Director of Finance.

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

- In the event that one or more of the City of Hermiston 's systems or applications are deemed corrupted or inaccessible, the City Manager and/or the Director of Finance will work with the respective vendor(s) and affected department heads to restore data from the most recent local backup and, if necessary, acquire replacement hardware.

- In the event that the location housing the City of Hermiston systems are no longer accessible, the City Manager and/or the Director of Finance will work with the respective vendor(s) and affected department heads 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 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 Finance.
- 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. 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.
- Clocks on network servers should be synchronized with the organization's other networking hardware using NTP or another means.

Network Segmentation

Network segmentation is used to limit access to data within the City of Hermiston network based upon data sensitivity. The City of Hermiston 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 city of Hermiston personnel and provides the user access to the intranet.

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

Protective Technology

Email Filtering

The City of Hermiston 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 be implemented to identify and quarantine emails that are deemed suspicious. This functionality may or may not be used at the discretion and/or approval of the Director of Finance in consultation with the third party network administrator.

Network Vulnerability Assessments

On at least an annual basis, the City of Hermiston will require/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 Finance 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 the third-party network administrator under the direction of the Director of Finance:

- 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 third party network administrator at least once per quarter. 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 appropriate measures to protect systems from malware and viruses. Real-time scanning will be enabled on all systems and weekly malware scans will be performed. A quarterly review of the anti-malware measures will be conducted by the Director of Finance and the third party network administrator to confirm the status of virus definition updates and scans.

Patch management

All software updates and patches will be distributed to all City of Hermiston systems 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 City of Hermiston'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 Hermiston 's information assets, can be defined as either an Electronic or Physical Incident.

The City Manager and/or the Director of Finance 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 Finance.
3. Contact the third-party service provider (and/or computer forensic specialist) as needed.

These 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.

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 and/or the Director of Finance.

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. 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.

The Director of Finance 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 the City of Hermiston'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 full-time and temporary/seasonal employees of the organization. This policy applies to all equipment that is owned or leased by the city of Hermiston. This policy is a supplement to the City of Hermiston Cybersecurity Policy.

1.0 Policy

The following actions shall constitute unacceptable use of the city 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 upon 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 of Hermiston 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 their respective supervisor or manager. Management investigates and responds to all reports of violations of the social networking policy and other related policies.
4. Only executive management is 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 Hermiston.
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 the City of Hermiston, except for “Concerted Activities.”
9. Employees must not reference the City of Hermiston or its services in the employee’s social medial posts, except for “Concerted Activities.”
10. City of Hermiston 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.

Maintaining Confidentiality

A significant amount of confidential customer information is maintained in paper-based form. All City of Hermiston employees 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. Ensure there are no confidential documents in open view if an employee is 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: 15 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 = 10 minutes

Portable Devices

The following Portable Devices are allowed for organization use only:

1. City of Hermiston issued 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 of Hermiston Cybersecurity Policy.

3.0 Reporting

Employees must report to the City Manager and/or the Director of Finance when they learn of a suspected breach of information or have lost a laptop, telephone, or USB memory with City of Hermiston 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 the **City of Hermiston** ("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: Mark Krawczyk

Director of Finance

Dated: _____

Receiving Party

By: _____

Printed Name: _____

Work Title: _____

Dated: _____

Appendix C - City of Hermiston Technology Data Breach Plan, Version 1.0

Objectives

The purpose of the Technology Data Breach Plan (TDBP) is to enable the City of Hermiston to respond effectively and efficiently to an actual or suspected data breach involving personally identifiable information (PII), confidential or protected information, identifiable information and other significant cybersecurity incident. The objectives of the TDBP are:

- Convene the Incident Response Team (IRT) as necessary.
- Validate and contain the data security breach.
- Analyze the breach to determine scope and composition.
- Minimize impact to the staff after a data breach has occurred.
- Notification of data owners, legal counsel, state/federal agencies and law enforcement as deemed necessary.

Planning Assumptions

The following planning assumptions were used in the development of TDBP:

- There may be data breaches that will have greater impact than others.
- There will be factors that are beyond the department's control or ability to predict during a data breach.
- City of Hermiston's data is backed up offsite daily.
- City of Hermiston's data is hosted by 3rd party providers.

Data Breach/Incident Response Team

The City of Hermiston has appointed the following people to the Data Breach/Incident Response Team (IRT): Assistant City Manager and Director of Finance for the city of Hermiston, IMESD Director of Information Technology, IMESD Assistant Director of Technology Operations, IMESD Assistant Director of Technology Information Systems, IMESD Network System Administrator, IMESD Server System Administrator. Additional members of the Inter-Mountain ESD administrative team and technology department may be designated to assist on the IRT

In the event the TDBP is activated, overall management of the response is delegated to this team. Their primary responsibilities include:

- Determine the nature of the data compromised and its impact to staff and the City itself.
- Communicate impact, the number of affected individuals, the likelihood information will be or has been used by unauthorized individuals and updates of progress to the City Manager.
- Coordinate with the Finance Director to ensure communication with staff as deemed appropriate.
- Oversight of the TDBP implementation and data breach resolution.
- Allocate and manage technology staff resources during the event.

- Work with vendors, 3rd party providers, manufacturers, legal counsel, state/federal agencies and law enforcement while correcting the data breach and its repercussions.
- Oversight of TDBP implementation debrief.

Activation

The TDBP will be activated in the event of the following:

- A data breach has occurred and affects the City itself. A data breach includes but is not limited to an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so.
- Personal Health Information (PHI) has been compromised.
- Personally Identifiable Information (PII) has been compromised.
- Confidential or sensitive data has been compromised.
- Network hack/intrusion has occurred.

The Information Security Officer (ISO) will act as the incident response manager (IRM). If the ISO is not able to act as the IRM, a member of the Administration will assume the role of IRM, with assistance from the IRT. The Director of Information Technology will work with the Director of Finance and the Assistant City Manager to dispense and coordinate the notification and public message of the breach.

Notification

The following groups will be notified in the event the plan has been activated:

- City Manager
- Department Heads

Information will be disseminated to the above groups through whichever means of communication deemed appropriate. This could include any one or combination of the following:

- Email
- Social Media
- Radio or Television
- First Class Mail
- Phone

The TDBP team will work with City leadership on which information will be conveyed to each above group, timing of that communication and what means will be used.

Implementation

The TDBP team has the following processes in place to contain the data breach in the least of amount of time possible:

- Data inventory of all systems containing sensitive data.

- Data dictionary of all hosted information systems.
- Maintained electronic documentation listing all server names, physical and virtual, and their function.
- Maintained electronic documentation of all local administrator accounts, passwords, and vendor contact information.
- The City's data backup solution includes the use of a backup manager and off-site file storage, which backs up data locally in the datacenter.

The following will take place during the incident response:

- The members of the IRT will be assembled once a breach has been validated.
- The IRT will determine the status of the breach, on-going, active, or post-breach. For an active and on-going breach, the IRT will initiate appropriate measures to prevent further data loss. These measures include, but are not limited to, securing and blocking unauthorized access to systems/data and preserving any and all evidence for investigation.
- The IRT will work with the data managers and data owners to determine the scope and composition of the breach, secure sensitive data, mitigate the damage that may arise from the breach and determine the root cause(s) of the breach to devise mitigating strategies and prevent future occurrences.
- The IRM will work with legal counsel and the Administration to determine an appropriate course of action pursuant to state statute. This includes notification of the authorities, local law enforcement, and the Missouri State Attorney General.
- Collaboration between the authorities and the IRT will take place with the IRM. The IRT will work with the proper authorities to make sure any and all evidence is properly handled and preserved.
- On advice from legal counsel, an outside party may be hired to conduct the forensic investigation of the breach. When the investigation has concluded, all evidence will be safely stored, recorded or destroyed (where appropriate).
- All affected data, machines and devices will be identified and removed from the network as deemed appropriate for the investigation. Interviews will be conducted with key personnel and facts of the incident will be documented and the evidence preserved for later examination.
- The IRT will work with the Communications department to outline the notification of the data owners and those affected. Communication will be sent out as directed by legal counsel and advised by the district communications team. The types of communication will include, but not limited to, email, text message, postal mail, substitute notice and/or phone call.
- The IRM, in conjunction with the IRT, legal counsel and Administration will determine if notification of affected individuals is necessary. If it is determined that identity theft or other fraud is not reasonably likely to occur as a result of the breach, such a determination shall be documented in writing and will be maintained for five years.

Deactivation

The TDBP team will deactivate the plan once the data breach has been fully contained.

Evaluation

Once the breach has been mitigated an internal evaluation of TDBP response will be conducted. The IRT, in conjunction with the IRM and others that were involved, will review the breach and all mitigation steps to determine the probable cause(s) and minimize the risk of a future occurrence. Feedback from the responders and affected entities will be incorporated into an after-action report and corrective action plan. The result will be an update to the TDBP and other emergency response plans as appropriate. Information security training programs will be modified to include countermeasures to mitigate and remediate previous breaches so that past breaches do not recur. The reports and incident review will be filed with all evidence of the breach.

Appendix D - City of Hermiston Technology Incident Recovery Plan, Version 1.0

Objectives

The primary purpose of the Technology Disaster Recovery Plan (TDRP) is to respond effectively and efficiently to a natural disaster or critical failure of the data center and/or core systems. The objectives during a natural disaster or critical failure are the following:

- Minimize the loss or downtime of core systems and access to business-critical data.
- Recover and restore critical systems and data.
- Maintain essential technology resources critical to the day-to-day operations.
- Minimize the impact to the staff during or after a critical failure.

Planning Assumptions

The following planning assumptions were used in the development of TDRP:

- There may be natural disasters that will have greater impact than others.
- There will be factors that are beyond the department's control or ability to predict during a disaster.
- There is the possibility of complete loss of the current data center.
- We will have adequate servers/storage to recover systems.
- City of Hermiston core servers/data is housed at the Police Dept. and backed up offsite to a NAS at City Hall.
- City of Hermiston data is also hosted by 3rd party providers.
- In the event of a critical failure to network infrastructure in the datacenter, networking may be significantly impacted.

Disaster Recovery/Critical Failure Team

City of Hermiston has appointed the following people to the disaster recovery/critical failure team: The Assistant City Manager and Director of Finance for the city of Hermiston, IMESD Director of Information Technology, IMESD Assistant Director of Technology Operations, IMESD Assistant Director of Technology Information Systems, IMESD Network System Administrator, IMESD Server System Administrator. Additional members of the InterMountain ESD administrative team and technology department may be designated to assist on the IRT

In the event the TDRP is activated, overall management of the response is delegated to this team. Their primary responsibilities include:

- Determining the impact of the natural disaster/critical failure.
- Communication of impact and or loss, and updates of progress to the City Manager and or the Director of Finance.
- Oversight of the TDRP implementation and restoration of critical systems and data.
- Allocation and management of technology staff during the event.
- Working with manufacturers and/or vendors during the recovery and restoration of critical systems and data.

Activation

The TDRP will be activated in the event of the following:

- A natural disaster has occurred and affects the operation of the data center. A natural disaster includes but is not limited to the following: tornado, earthquake, lightning, and flood.
- A fire has impacted the data center.
- Water or flooding has impacted the data center.
- Critical system failure.

The Information Security Officer (ISO) will act as the incident response manager (IRM). If the ISO is not able to act as the IRM, a member of the Administration will assume the role of IRM, with assistance from the IRT.

Notification

The following groups will be notified in the event the plan has been activated:

- City Manager
- Department Heads

Information will be disseminated to the above groups through whichever means of communication is available at the time. This could include any one or combination of the following:

- Phone
- Email
- Social Media
- Radio or Television

The TDRP team will work with leadership on which information will be conveyed to each above group and what means will be used.

Implementation

The TDRP team has the following in place to bring the City back online in the least of amount of time possible:

- Maintained electronic documentation listing all server names, physical and virtual, and their function.
- Maintained electronic documentation of all local administrator accounts, passwords, and vendor contact information.
- The City's data backup solution includes the use of a backup manager and off-site file storage, which backs up data locally in the datacenter.
- In the event of a critical system failure, the City can restore that server back to a new environment from the backup solution.

Deactivation

The TDRP team will deactivate the plan once services are fully restored.

Evaluation

An internal evaluation of TDRP response will be conducted. This will entail gathering documentation from the response and feedback from all stakeholders and incorporate into an after-action report and corrective action plan. The result will be an update to the TDRP and other emergency response plans as appropriate.