

April 11, 2023

Honorable Michael D. Coughlan, Presiding Judge
San Joaquin County Superior Court
180 East Weber Avenue, Suite 1306J
Stockton, CA 95202

Re: Followup Response to Grand Jury Final Report Case No. 0321 (2021/2022).

Honorable Michael D. Coughlan,

This letter is provided to the Grand Jury as a followup response to the City of Lathrop response to Grand Jury Final Report for Case No. 0321 (2021/2022). At its regularly scheduled City Council Meeting on April 10, 2023, the City Council of the City of Lathrop reviewed and approved the policies described herein and directed me to write this letter of response on their behalf.

The 2021/2022 Grand Jury Final Report for Case No. 0321 stated the following:

Grand Jury Finding F3.3: "The City of Lathrop does not have an approved Business Continuity Plan, rendering the City relatively unprepared to restore essential services in a disruptive event."

Grand Jury Recommendation R3.3: "By January 1, 2023, the Lathrop City Council, in conjunction with the City's IT department, develop, adopt and implement a Business Continuity Plan."

City Council Original Response: The City of Lathrop has an unwritten Business Continuity Plan but not a written one. The City of Lathrop City Council agrees with Grand Jury Finding F3.3 and Recommendation R3.3 and documentation is anticipated to be complete by January of 2023.

Followup Response: The City worked with its consultant on the development and standardization of the City's unwritten Business Continuity Plan. Because those policies include confidential details that would allow a potential hacker to gain easier access to the City's Information Technology resources, those were shared confidentially with the Grand Jury on March 28,

2023 and Council adopts the same in compliance with the Grand Jury's recommendation. Redactions on the attached Business Continuity-Disaster Recovery Plan are intended to protect security information.

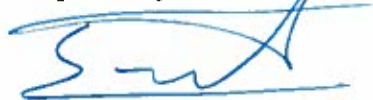
Grand Jury Finding F3.4: "The City of Lathrop does not have a formal internal policy or procedure to address ransomware attacks. This absence of policy could cause confusion, delay and greater loss of security in the event of such an attack."

Grand Jury Recommendation R3.4: "By November 1, 2022, the Lathrop City Council, in conjunction with the City's IT department, develop, adopt and implement a formal internal policy and procedure for a ransomware attack."

City Council Original Response: The City of Lathrop has an unwritten, internal procedure to address ransomware attacks and, in addition to such, has hired a consultant whom will assist the City in development and implementation of a formal written policy for procedures to address ransomware attacks. The City of Lathrop City Council agrees with Grand Jury Finding F3.4 and Recommendation R3.4 and anticipates documentation will be complete by January of 2023.

Followup Response: The City worked with its consultant on the development of the City's unwritten, internal procedures to address ransomware attacks and standardize those into internal policies. Because those policies include confidential details that would allow a potential hacker to gain easier access to the City's Information Technology resources, those were shared confidentially with the Grand Jury on March 28, 2023 and Council adopts the same in compliance with the Grand Jury's recommendation. Redactions on the attached Information Security Policy and the inclusion of only the Executive Summary and Introduction of the Incident Response Plan are intended to protect security information.

Respectfully submitted,



Salvador V. Navarrete
City Attorney

SVN/trb

Enclosures

Cc: Trisa Martinez, Grand Jury Staff Secretary, San Joaquin County Superior Court via email at grandjury@sjcourts.org



City of Lathrop Business Continuity-Disaster Recovery Plan

Version History

Version	Date	Author	Reason/Comments
1.5	March 2023		Document Origination



Table of Contents

City of Lathrop Business Continuity-Disaster Recovery Plan	1
Version History.....	1
Table of Contents	2
Part I	3
Introduction	3
Part II	4
Design of the Plan	4
Contact Information.....	7
Part III	8
Roles and Responsibilities.....	8
Chief Information Officer (CIO).....	8
Business Continuity Management Team (BCMT)	8
Part IV	10
Business Continuity Framework.....	10
Phase I – Disaster Detection and Determination.....	10
Phase II – Notification of Personnel Responsible for Recovery	11
Phase III – Initiate the Business Continuity Plan	11
Phase IV - Disaster Recovery Strategy	12
Scope of the Business Continuity Plan.....	13
Information Systems listed by Risk Category.....	14



Part I

Introduction

Planning for the business continuity of City of Lathrop in the aftermath of a disaster is a complex task. Preparation for, response to, and recovery from a disaster affecting the business functions of the City of Lathrop requires the cooperative efforts of the Business Continuity Team (BCT) in partnership with the essential departments of the City of Lathrop. This document records the Plan that outlines and coordinates these efforts, reflecting the analyses by the City of Lathrop Chief Information Officer, Tony Fernandes.

The purpose of the City of Lathrop Business Continuity-Disaster Recovery Plan is to allow City of Lathrop to respond quickly and appropriately to service interrupting incidents.

Event Definition

Adverse Events Definition

How to Use This Document

Use this document to learn about the issues involved in planning for the continuity of the critical and essential business functions at City of Lathrop, for training personnel, and for recovering from a disaster. This document is divided into four parts, as described below.

Part Contents

Part I - Information about the document itself.

Part II - Design of the Plan that this document records, including information about the overall structure of business continuity planning at City of Lathrop.

Part III - General responsibilities of the individual City of Lathrop Support Teams that together form the Business Continuity Management Team, emphasizing the function of each team and its preparation responsibilities.

Part IV - Recovery actions for the City of Lathrop Support Teams and important checklists such as the notification list for a disaster and an inventory of resources required for the environment. (Note: If a "disaster" situation arises, Section IV of the Plan is the only section that needs to be referenced. It contains all the procedures and support information for recovery.



Audience

This document addresses several groups within the City of Lathrop central administration with differing levels and types of responsibilities for business continuity, as follows:

- Administration
- Business Continuity Management Team (BCMT)
- City of Lathrop Business Continuity Team (BCT)
- External Organizations

It should be emphasized that this document is addressed particularly to the members of the Business Continuity Management Team, since they have the responsibility of preparing for, responding to, and recovering from any disaster that impacts City of Lathrop. Part III of this document describes the composition of the Business Continuity Management Team in detail.

Distribution

As the written record of City of Lathrop's Business Continuity Plan, this document is distributed to each member of the Business Continuity Management Team.

It is also distributed to City of Lathrop Department Heads and other Community Organizations and while not primarily involved with the direct recover effort, will require advanced knowledge of planned actions and needs. Community Organizations include Physical Plants, security provided by the Police, and service provided by the Fire Department.

Part II

Design of the Plan

Part II describes the philosophy of business continuity planning at City of Lathrop generally, and the kind of analysis that produced this Plan. It also provides an overview of the functions of the Business Continuity Management Team in implementing this Plan.

Purpose

City of Lathrop increasingly depends on computer-supported information processing and telecommunications. The increasing dependency on computers and telecommunications for operational support poses the risk that a lengthy loss of these capabilities could seriously affect the overall business performance of the City of Lathrop.



City of Lathrop Information Services Department recognizes the low probability of severe damage to data processing telecommunications and computer information systems. Nevertheless, because of the potential



impact to City of Lathrop, [REDACTED]

The Business Continuity Plan (BCP) identifies the critical functions of the City of Lathrop and the resources required to support them. The BCP provides guidelines for ensuring that needed personnel and resources are available for both disaster preparation and response and that the proper steps will be carried out to permit the timely restoration of services.

This BCP specifies the responsibilities of the Business Continuity Management Team, whose mission is to establish City of Lathrop level procedures to ensure the continuity of City of Lathrop 's business functions. In the event of a disaster affecting any of the functional sites, the Business Continuity Management Team serves as liaison between the functional site(s) affected and other community organizations providing major services. These services include the support provided by Physical Plants, security provided by the Police, service provided by the Fire Department, and public information dissemination handled by the City of Lathrop Communications Team, among other.

Assumptions

The City of Lathrop Plan is predicated on the validity of the following three assumptions:

[REDACTED]

It should be noted however, that the Plan will still be functional and effective even in an area-wide disaster. [REDACTED]

[REDACTED]

[REDACTED]

- The Plan is a document that reflects the changing environment and requirements of City of Lathrop. Therefore, the Plan requires the continued allocation of resources to maintain it and to keep it in a constant state of readiness.

Development

City of Lathrop 's Chief Information Officer is responsible for developing the City of Lathrop 's Business Continuity Plan. Development and support of individual City of Lathrop Department Plans are the responsibility of the Department Heads planning for recovery.



Maintenance

Ensuring that the Plan reflects ongoing changes to resources is crucial. This task includes updating the Plan and revising this document to reflect updates; testing the updated Plan; and training personnel. The Business Continuity Management Team Coordinators are responsible for this comprehensive maintenance task.

The Business Continuity Management Team Coordinators ensures that a formal review is initiated whenever there is a significant change required for the plan. Annually, the Business Continuity Management Team Coordinators initiates a complete review of the Plan, which could result in major revisions to this document. These revisions will be distributed to all authorized personnel, who exchange their old plans for the newly revised plans. At that time the Coordinators will provide an annual status report on continuity planning to the City of Lathrop Chief Information Officer.

Testing





Contact Information[†]

Updated March 2023

Name	Title	Role	Contact Information	Escalation (1-3)*
	Business Continuity Management Team Coordinator	BC manager		
	Infrastructure Manager	BC Manager		
	CIO	CIO		
	Communications Manager	BCMT member		
	Legal	BCMT member		
	Risk Manager	BCMT member		
	HR Representative	BCMT member		
	Physical Security Representative	BCMT member		
	3 rd Party Network Support			
FBI	Regulatory/Government Reporting Body			

*Escalation level determines order in which notification should occur:

1. Notify first, required on all incidents
2. Required on all moderate or high-severity incidents
3. Involve as needed

[†]This information may be revised from time to time, as internal City personnel and external organizations change. For the most up to date copy, please see *Contact Information* located in *Appendix I: Supporting Document List*.



Part III

Roles and Responsibilities

Chief Information Officer (CIO)

- Seek approval from City Manager for the administration of the Business Continuity Program.
- Coordinate response activities with department heads and external resources as needed to minimize damages to information resources.
- Provide updates on response activities to Business Continuity Management Team (BCMT) and other stakeholders during an incident.
- Ensure service level agreements with service providers clearly define expectations of the organization and the service provider in relation to Business Continuity.
- Ensure policies related to recovery management accurately represent the goals of the City of Lathrop.
- Review the Business Continuity Plan ("the Plan") to ensure that it meets policy objectives and accurately reflects the goals of the City.
- Ensure Cyber Insurance is maintained as necessary and appropriate stakeholders are informed.
- Ensure lessons learned are applied/weighed based on risk for Business Continuity incidents.

Business Continuity Management Team (BCMT)

Under the overall direction of the Business Continuity Manager, support is provided to assist City of Lathrop functional site's recovery by the Business Continuity Team members and external vendors. These teams work the problem condition to restore services and provide assistance at the City of Lathrop level. Support from external vendors is generally documented in a procedure's manual for the City of Lathrop. The Business Continuity Plan is an adjunct to that documentation and highlights the interfaces between the vendor level service and the Business Continuity Team operations requirements. In cases where the documentation in this Plan and the vendor's documents differ, the vendor's documentation has precedence.

- Advise on recovery response activities relevant to their area of expertise.
- Maintain a general understanding of the Plan and policies of the City of Lathrop.
- Ensure business continuity activities are in accordance with legal, contractual, and regulatory requirements.
- Participate in tests of the Business Continuity plan and procedures.
- Responsible for internal and external communications pertaining to recovery activities.

Business Continuity Manager

The Business Continuity manager oversees and prioritizes actions during the incident. They are also responsible for conveying the special requirements of high severity activities to the rest of the City of Lathrop personnel. Additionally, they are responsible for understanding the SLAs in place with third party vendors, and the role third parties may play in specific response scenarios.

Further responsibilities:

- Assemble a Business Continuity Response Team (CSIRT).
- Ensure personnel tasked with business continuity responsibilities are trained and knowledgeable on how to respond to incidents.



- Update Business Continuity Plan and procedures as needed [REDACTED]
- [REDACTED]
- Initiate tests of the business Continuity Plan [REDACTED]
- Ensure team activities comply with legal and industry requirements for Business Continuity procedures.
- Act as the primary Business Continuity Manager, responsible for declaring a disaster incident, managing team response activities, and approving close of recovery incidents.
- [REDACTED]

Business Continuity Team Members

The Business Continuity Manager is supported by a team of technical staff that work directly with the affected information systems to restore service to end users. Team members are typically comprised of subject matter experts (SMEs), senior level IT staff, third parties, outsourced security, or forensic partners.

Teams and responsibilities:

- **Damage Assessment/Salvage Team.** Headed by the Infrastructure Manager and activated during the initial stage of an emergency, the team reports directly to the Business Continuity Management Team, evaluates the initial status of the damaged functional area, and estimates both the time to reoccupy the facility and the salvageability of the remaining equipment. [REDACTED]

- **Transportation Team.** A temporary City of Lathrop Support Team headed jointly by the Infrastructure Manager and Physical Security Representative responsible for transporting resources, personnel, equipment, and materials to back-up sites as necessary.
- **Telecommunications Team.** Headed by the Infrastructure Manager is responsible for establishing voice and data communications between the affected site and the City of Lathrop.



TABLE 1: CITY OF LATHROP BUSINESS CONTINUITY TEAM MEMBERS*

Updated March 2023

No.	BCT Member	Role
1		Business Continuity Manager
2		Network SME
3		Network SME
4		Senior IT Staff
5		Systems Engineer
6		Business Continuity Team Member - Recorder
7		Business Continuity Team Member - Recorder

* This information may be revised from time to time, as internal City personnel and external organizations change. For the most up to date copy, please see Table 1: City of Lathrop Business Continuity Team Members located in Appendix I: Supporting Document List.

Part IV

Business Continuity Framework



4. Disaster Recovery Strategy



Each subsection below identifies the organization(s) and/or position(s) responsible for each of these responses.

Phase I – Disaster Detection and Determination





Phase II – Notification of Personnel Responsible for Recovery

When a situation occurs that could result in interruption of processing

- The Business Continuity Manager¹
- The Business Continuity Team¹

¹ Refer to page 7, Contact Information

Phase III – Initiate the Business Continuity Plan

Initiation of this Plan is the responsibility of the Business Continuity Management Team Coordinator or any member of the Business Continuity Management Team.

Activation of a Designated Hot Site

- Hot Site:

The responsibility for activating any of the designated hot sites or back-up resources is delegated to Chief Information Officer (CIO). In the absence of the CIO, responsibility reverts to the Communications Manager. The CIO, or alternate, determines Infrastructure Manager and Communications Manager.

Dissemination of Public Information

The Communications Manager is responsible for directing all meetings and discussions with the news media and the public, and in conjunction with the BCT Manager and necessary BCT personnel not actively participating in the recovery operation. In the absence of the Communications Manager, the responsibility reverts to the senior official present at the scene.

Recovery Status Information Number

ISD Helpdesk; is the predefined number established as the voice mail information number for posting recovery status and information notices.



Provision of Support Services to Aid Recovery

During and following a disaster, at the direction of the CIO, each department head shall have their respected department personnel available [REDACTED]

Phase IV - Disaster Recovery Strategy

The disaster recovery strategy explained below [REDACTED]

[REDACTED] Subsections below explain the context in which the City of Lathrop's Business Continuity Plan operates.

This section addresses three phases of disaster recovery:

1. [REDACTED]
2. [REDACTED]
3. [REDACTED]

Emergency Phase

The emergency phase begins with the initial response to a disaster. During this phase, the existing emergency plans and procedures are implemented for direct efforts to protect life and property. Security over the area is established as local support services such as the Police and Fire Departments are enlisted through existing mechanisms. The Business Continuity Manager is alerted and begins to monitor the situation.

[REDACTED]

[REDACTED]

[REDACTED]



Back-up Phase

[REDACTED]

[REDACTED]

Recovery Phase

The time required for recovery of the functional site and the eventual restoration of normal processing depends on the damage caused by the disaster.

[REDACTED] The primary goal is to restore normal operations as soon as possible.

Scope of the Business Continuity Plan

The object of this Plan

[REDACTED]

[REDACTED]

[REDACTED]

Note:

[REDACTED]

[REDACTED]



Table 7: Categorization of Federal Information and Information Systems



Information Systems listed by Risk Category (Deliverable Pending)



Appendix I: Supporting Document List

The following documents have been defined to assist in incident response for the City of Lathrop.

Document	URL
<u>Contact Information</u>	
<u>Table 1: City of Lathrop Business Continuity Team Members</u>	



Contact Information

Updated March 2023

Name	Title	Role	Contact Information	Escalation (1-3)*
	Business Continuity Management Team Coordinator	BC manager		
	Infrastructure Manager	BC Manager		
	CIO	CIO		
	Communications Manager	BCMT member		
	Legal	BCMT member		
	Risk Manager	BCMT member		
	HR Representative	BCMT member		
	Physical Security Representative	BCMT member		
	3 rd Party Network Support			
FBI	Regulatory/Government Reporting Body			

*Escalation level determines order in which notification should occur:

1. Notify first, required on all incidents
2. Required on all moderate or high-severity incidents
3. Involve as needed



Table 1: City of Lathrop Business Continuity Team Members

Updated March 2023

No.	BCT Member	Role
1		Business Continuity Manager
2		Network SME
3		Network SME
4		Senior IT Staff
5		Systems Engineer
6		Business Continuity Team Member - Recorder
7		Business Continuity Team Member - Recorder



Information Security Policy

City of Lathrop Information Security Policy

Version History

Version	Date	Author	Reason/Comments
1.8	March 2023		Document Origination



Information Security Policy

Table of Contents

City of Lathrop Information Security Policy	1
Version History	1
Table of Contents	2
Introduction	4
Contact Information*	5
Roles and Responsibilities	6
Chief Information Officer (CIO)	6
Cyber Security Information Security Team (CSIST)	6
CSIST Commander	6
Information Security Team Members*	7
Information Security Framework	8
Phase I – Organizational Security	8
Phase II – Functional Responsibilities	8
Phase III – Separation of Duties	11
Phase IV – Information Risk Management	11
Phase V – Information Classification and Handling	11
Phase VI – Information Sharing	12
Phase VII – IT Asset Management	14
Phase VIII – Personnel Security	14
Phase IX – Information Security Incident Management	15
Phase X – Physical and Environmental Security	16
Phase XI – Account Management and Access Control	16
Phase XII – System Security	18
Phase XIII – Collaborative computing Devices	20
Phase XIV – Vulnerability Management	21
Phase XV – Operations Security	21
Reference	24
Appendix I: Security Awareness References	24
Acceptable Use of Technology 00-17	26
Vendor Remote Log-In Questionnaire	32
Computer Setup Checklist	33



Information Security Policy

Contact Information	34
Information Security Team Members	35



Information Security Policy

Introduction

This policy defines the mandatory minimum information security requirements as defined below under Scope. Any department within the City of Lathrop may, based on its individual business needs and specific legal and federal requirements, exceed the security requirements put forth in this policy, but must, at a minimum, achieve the security levels required by this policy.

Scope

This policy applies to all employees, consultants, contractors, and vendors working on behalf of the City, that use or access any IT resource for which the City of Lathrop has administrative responsibility. While a vendor may adopt a different policy, it must include the requirements set forth in this one.

This policy encompasses all systems, automated and manual, for which the organization has administrative responsibility, including systems managed or hosted by vendors on behalf of the organization.

Information

This policy acts as an umbrella document to all other security policies and associated standards. This policy defines the responsibility of all employees, consultants, contractors, and vendors working on behalf of the City to:

- protect and maintain the confidentiality, integrity, and availability of information and related infrastructure assets;
- manage the risk of security exposure or compromise;
- ensure a secure and stable information technology (IT) environment;
- identify and respond to events involving information asset misuse, loss, or unauthorized disclosure;
- monitor systems for anomalies that might indicate compromise; and
- promote and increase the awareness of information security.

Failure to secure and protect the confidentiality, integrity, and availability of information assets in today's highly networked environment can damage or shut down systems that operate critical infrastructure, financial and business transactions, and compromise data which could result in legal and regulatory non-compliance.

Compliance

This policy shall take effect upon publication. Policies and standards may be amended at any time as see fit by the Chief Information Officer (CIO).

City of Lathrop employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-City employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

Exceptions

No exceptions to this policy will be approved.



Information Security Policy

Contact Information⁺

Listed personnel that should be contacted in the event of data loss incidents.

Updated March 2023

Name	Title	Role	Contact Information	Escalation (1-3)*
	Information Security Risk Coordinator	CSIST Commander		
	Asset Manager	CSIST Commander		
	Infrastructure Manager	CSIST Manager		
	CIO	CIO		
	Communications Manager	CSIST member		
	Legal	CSIST member		
	Risk Manager	CSIST member		
	HR Representative	CSIST member		
	Physical Security Representative	CSIST member		
	3 rd Party Support			
FBI	Regulatory/Government Reporting Body			

*Escalation level determines order in which notification should occur in the event of a data loss incident:

1. Notify First, required on all incidents
2. Required on all moderate or high-severity incidents
3. Involve as needed

⁺This information may be revised from time to time, as internal City personnel and external organizations change. For the most up to date copy, please see *Contact Information* located in *Appendix I: Reference*.



Information Security Policy

Roles and Responsibilities

Chief Information Officer (CIO)

- Ensure service level agreements with service providers clearly define expectations of the organization and the service provider in relation to hardware and software.
- Ensure policies related to Information Security accurately represent the goals of the city.
- Ensure Cyber Insurance is maintained as necessary and appropriate stakeholders are informed.
- Establish and maintain a security team and function with the ability to identify, protect, detect, respond, and recover from attacks against City information resources.
- Develop and maintain a centralized incident response plan capable of addressing major compromises of City information resources.

Cyber Security Information Security Team (CSIST)

- Consists of legal experts, risk managers, and other department managers that may be consulted or notified during data documentation and policy creation.
- **Advise on Information Security policy activities relevant to their area of expertise.**
- Ensure Information Security activities are in accordance with legal, contractual, and regulatory requirements.
- Responsible for internal communications pertaining to Information Security.

CSIST Commander

Cyber Security Information Security Team Commander oversees development and is responsible for implementing and monitoring the Information Security Plan. Managing and approving the Service Level Agreements (SLAs) in place with third parties, and the role third parties may play in Information Security.

Further responsibilities:

- Assemble a Cyber Security Information Security Team (CSIST).
- Ensure personnel tasked with Information Security responsibilities are trained and knowledgeable on how to perform Asset documentation and maintenance.
- Update security policies as needed [REDACTED]
- Review the security policies [REDACTED]
- Ensure team activities comply with legal and industry requirements for Information Security procedures.
- Act as the primary Asset Manager, responsible for Asset integrity and confidentiality, managing team response activities.
- Be aware of Cyber Insurance Policies, contact mechanisms, and when to initiate Cyber Incident Response Team Notification.



Information Security Policy

Information Security Team Members[†]

Updated March 2023

The Asset Manager (tf) is supported by a team of technical staff that work directly with Information systems to configure, perform, and document assets.

Further responsibilities:



No.	CSIRT Member	Role
1		CSIST Commander
2		Network Subject Matter Expert
3		Network Subject Matter Expert
4		Senior IT Staff
5		Systems Engineer
6		Recorder
7		Recorder

[†]This information may be revised from time to time, as Internal City personnel and external organizations change. For the most up to date copy, please see *Information Security Team Members* located in *Appendix I: Reference*.



Information Security Policy

Information Security Framework

Phase I – Organizational Security

Information security requires [REDACTED] and an information technology security function. It is recommended that the functions be performed [REDACTED]

1. The Information Security Risk Coordinator is responsible to certify that information risk management functions are met, ensuring that:

i. risk-related considerations for information assets and individual information systems, including authorization decisions, are viewed wholly from the perspective of the City of Lathrop regarding the overall strategic goals and objectives of the City of Lathrop in carrying out its core missions and business functions; and

ii. the management of information assets, [REDACTED]

mission/business success.

2. The Information Security Risk Coordinator is responsible to certify that information technology security functions are met. [REDACTED]

Phase II – Functional Responsibilities

The City of Lathrop CIO is responsible for:

2. identifying City of Lathrop information security responsibilities and goals and integrating them into relevant processes;

3. supporting the consistent implementation of information security policies and standards;

4. supporting security within the City of Lathrop through clear direction and demonstrated commitment of appropriate resources.

5. promoting awareness of information security best practices through the regular dissemination of materials provided by the Information Security Risk Coordinator (tf);



Information Security Policy

6. Implementing a process for determining information classification and categorization, based on industry recommended practices, State directives, and legal and regulatory requirements, to determine the appropriate levels of protection for that information; (*Appendix I: Security Awareness References. FIPS 199 Standards for Security Categorization of Federal Information and Information Systems*).
7. implementing the process for information asset identification, handling, use, transmission, and disposal based on information classification and categorization;
8. determining who, within the City of Lathrop, will be assigned and serve as information owners while maintaining ultimate responsibility for the confidentiality, integrity, and availability of the data;
9. participating in the response to security incidents;
10. complying with applicable notification requirements in the event of a breach of private information;
11. adhering to specific legal and regulatory requirements related to information security;
12. communicating the requirements of this policy and the associated standards, including the consequences of non-compliance, to the City of Lathrop workforce and third parties, and addressing adherence in third party agreements.

The City of Lathrop Information Security Risk Coordinator (tf) is responsible for:

1. maintaining familiarity with the City of Lathrop business functions and requirements;
2. maintaining an adequate level of current knowledge and proficiency in information security through annual Continuing Professional Education (CPE) credits directly related to information security;
3. assessing City of Lathrop compliance with information security policies and legal and regulatory information security requirements;
4. evaluating information security risks and assisting the City of Lathrop in understanding its information security risks and how to appropriately manage those risks;
5. representing and ensuring security architecture considerations are addressed;
6. advising on security issues related to procurement of products and services;



Information Security Policy

7. escalating security concerns that are not being adequately addressed according to the applicable reporting and escalation procedures;
8. disseminating threat information to appropriate parties;
9. participating in the response to potential security incidents;
10. participating in the development of enterprise policies and standards that consider the City of Lathrop needs; and
11. promoting information security awareness.

The City of Lathrop Infrastructure Manager (tf) is responsible for:

1. supporting security by providing clear direction and consideration of security controls in the data processing infrastructure and computing network(s) which support the information owners;
2. providing resources needed to maintain a level of information security control consistent with this policy;
3. identifying and implementing all processes, policies, and controls relative to security requirements defined by the City of Lathrop business and this policy;
4. implementing the proper controls for information owned by the City of Lathrop based on the City of Lathrop classification designations;
5. providing training to appropriate technical staff on secure operations (e.g., secure coding, secure configuration);
6. fostering the participation of information security and technical staff in protecting information assets, and in identifying, selecting, and implementing appropriate and cost-effective security controls and procedures; and
7. implementing business continuity and disaster recovery plans

The City of Lathrop workforce is responsible for:

1. understanding the baseline information security controls necessary to protect the confidentiality, integrity, and availability of information entrusted to City of Lathrop;
2. protecting City of Lathrop information and resources from unauthorized use or disclosure;
3. protecting personal, private, sensitive information (PPSI) from unauthorized use or disclosure;



Information Security Policy

4. abiding by City of Lathrop Policy, Acceptable Use of Information Technology Resources (*Appendix I: Security Awareness References. Acceptable Use of Technology 00-17*).
5. reporting suspected information security incidents or weaknesses to the appropriate manager and designated security representatives.

Phase III – Separation of Duties

The City of Lathrop shall maintain:



Phase IV – Information Risk Management

The City of Lathrop shall maintain:



- b. Risk assessments are required for new projects, implementations of new technologies, any significant updates, or changes to the operating environment, or in response to the discovery of significant vulnerabilities. Risk assessments are required regardless if the work is done by City of Lathrop, vendor/contractor, or any other third party on behalf of the City of Lathrop.



- c. Risk assessment results, and the decisions made based on these results, must be documented.

Phase V – Information Classification and Handling

The City of Lathrop shall maintain:

- a. All information, which is created, acquired, or used in support of City of Lathrop business activities, must only be used for its intended business purpose.



Information Security Policy

- b. All information assets must have an information owner established by the City of Lathrop's Information Services Department (ISD).
- c. Information must be properly managed from its creation, through authorized use, to proper disposal.
- d. All information assets must be reviewed [REDACTED]
[REDACTED] Any changes to the individual data elements of an information asset requires an immediate review by the CIO.

[REDACTED]

- f. If the City of Lathrop [REDACTED]

[REDACTED]

- h. All reproductions of information in its entirety must carry the same confidentiality category as the original. Partial reproductions need to be evaluated by the CIO to determine if a new category is warranted.

- i. Each category has an approved set of baseline controls designed to protect the data asset and [REDACTED]

[REDACTED]

- j. The City of Lathrop must communicate the requirements for secure handling of information to its workforce.

[REDACTED]

Phase VI – Information Sharing

The City of Lathrop content made available to the general public must be reviewed by the City of Lathrop Attorney's office, defined and approved according to the Public Records Act (PRA). The process must include the review and approval of updates to publicly available content and must consider the type and classification of information posted:



Information Security Policy

[REDACTED]

b. For non-public information to be released outside the City of Lathrop or shared between the City of Lathrop and external entities, a process must be established that, at a minimum:

1. ensures that an information categorization has been performed and documented for the information to be released or shared;
2. documents the intended use of the information;
3. identifies the responsibilities of each party for protecting the information;
4. defines the process and minimum controls required to transmit, store, and use the information;
5. records the measures that each party has in place to protect the information;
6. defines a method for compliance measurement;
7. provides a signoff procedure for each party to accept responsibilities,
8. establishes a schedule and procedure for reviewing the controls; and
9. identifies an end date for the use of the information (if applicable).

c. In addition to the requirements in Phase VI Section b, when information categorized as having a High-Impact Confidentiality requirement is to be released or shared, the City of Lathrop Attorney's office must ensure that they:

1. have a formal written agreement (e.g., Non-Disclosure Agreement (NDA), Acceptable Use Policy, Memorandum of Understanding (MOU), etc.), which contains the requirements for the handling of information, in place prior to sharing that information with any other third-party.
2. designate the level of management who can give written approval for:





Information Security Policy

Phase VII – IT Asset Management

The City of Lathrop shall maintain:

- a. All IT hardware and software assets must be assigned by the City of Lathrop Information Services Department (ISD) to a designated business unit or individual within the City of Lathrop for its use, however the asset continues to be owned by ISD.
- b. The City of Lathrop ISD are required to maintain an inventory of hardware and software assets, including all system components (e.g., network address, machine name, software version) at a level of granularity deemed necessary for tracking and reporting.

Phase VIII – Personnel Security

The City of Lathrop shall maintain:

- a. The City of Lathrop workforce must receive general information security awareness training, to include recognizing and reporting insider threats, within 30 days of hire. Additional training on City of Lathrop specific information security procedures, if required, must be completed before access is provided to specific City of Lathrop sensitive information not covered in the general information security training. All information security training must be reinforced at least annually and must be tracked by the City of Lathrop Information Systems Department (ISD).
- b. The City of Lathrop must require the workforce to abide by the following policies:
 - i. Policy 00-15, Cellular and Personal Digital Assistant
 - ii. Policy 00-16, Password Control
 - iii. Policy 00-17, Acceptable Use of Technology
 - iv. Policy 00-18, Automatic Logoff Policy
 - v. Policy 00-19, Physical Entry Control Security
 - vi. Policy 00-20, User Account
 - vii. Policy 00-21, Workstation Security
 - viii. Policy 00-22, Data Backups
 - ix. Policy 00-23, IT Helpdesk
 - x. Policy 00-24, Operations and Fault Logs
 - xi. Policy 00-25, Security Device and Media Control
 - xii. Policy 00-26, Website Links
 - xiii. Policy 00-27, Website Policy
 - xiv. Policy 00-28, Television Broadcast
 - xv. Policy 00-29, Social Media
 - xvi. Policy 00-30, Video Monitoring and Retention
 - xvii. Policy 00-31, Remote Working



Information Security Policy

- c. All job positions must be evaluated by the City of Lathrop Human Resources (HR) department along with approval by the direct department head to determine whether they require access to sensitive information and/or sensitive information technology assets.
- d. For those job positions requiring access to sensitive information and sensitive information technology assets, the City of Lathrop CIO must conduct workforce suitability determinations, unless prohibited from doing so by law, regulation, or contract. Depending on the risk level, suitability determinations may include, as appropriate and permissible, evaluation of criminal history record information or other reports from federal, state, and private sources that maintain public and non-public records. The suitability determination must provide reasonable grounds for the City of Lathrop CIO to conclude that an individual will likely be able to perform the required duties and responsibilities of the subject position without undue risk to the City of Lathrop.
- e. A **process** must be established within the City of Lathrop to repeat or review suitability determinations periodically and upon change of job duties or position.
- f. City of Lathrop employees are responsible for ensuring all City of Lathrop issued property is returned to HR prior to an employee's separation.
- g. City of Lathrop ISD are responsible for ensuring accounts are disabled and access is removed immediately upon notification from HR of an employee's separation from the City of Lathrop.
- h. HR is responsible for providing ISD proper notification of each employee's separation from the City of Lathrop.
 - i. For sensitive positions, HR will provide notification to ISD prior to an employee's separation from the City of Lathrop.
 - ii. For non-sensitive positions, HR will provide notification to ISD within ten (10) minutes of an employee's separation from the City of Lathrop
- i. Within 24 hours, each department is responsible to provide ISD a Technical Service Request (TSR) with instructions on archiving or deleting the separated employee's data, which includes emails.

Phase IX – Information Security Incident Management

City of Lathrop must have an incident response plan, consistent with NIST standards, to effectively respond to information security incidents.

- a. All observed or suspected information security incidents or weaknesses are to be reported the City of Lathrop Information Services Department (ISD) as quickly as possible. If a member of the workforce feels that information security concerns are not being appropriately addressed, they may confidentially contact the CIO directly.



Information Security Policy

- b. The Cyber Security Incident Response Team must be notified incident [REDACTED]

Phase X – Physical and Environmental Security

The City of Lathrop shall maintain:

- [REDACTED]
- b. An annual risk assessment must be performed by ISD for information processing and storage facilities to determine whether existing controls are operating correctly and if additional physical security measures are necessary.
- c. Information technology equipment must be physically protected from security threats and environmental hazards. Special controls may also be necessary to protect supporting infrastructure and facilities such as electrical supply and cabling infrastructure.
- d. All information technology equipment and information media must be secured [REDACTED]
- e. Visitors to information processing and storage facilities, including maintenance personnel, must be always escorted. Any maintenance performed remotely must be virtually escorted.
- f. For City of Lathrop information that has a High Confidentiality requirement, software or automated processes must be implemented to keep track of individual electronic documents and files, devices, or media and the individuals who have possession of them. City of Lathrop information is currently monitored by [REDACTED]

Phase XI – Account Management and Access Control

The City of Lathrop shall maintain:

- a. All accounts must have an individual employee or group assigned to be responsible for account management [REDACTED]
- b. Access to systems must be provided through the use of individually assigned, unique identifiers known as user-IDs.
- c. Associated with each user-ID is an authentication token (e.g., password) which must be used to authenticate the identity of the person or system requesting access.



Information Security Policy

d. Automated techniques and controls must be implemented to lock a session and require authentication or re-authentication after a period of inactivity for any system where authentication is required. Information on the screen must be replaced with publicly viewable information (e.g., screen saver, blank screen, clock) during the session lock.

e. Automated techniques and controls must be implemented to terminate a session after specific conditions are met. Specific conditions include:

1. *Group Policy rule will be implemented that terminates session [REDACTED] inactivity.*

f. Tokens used to authenticate a person or process must be treated as confidential and protected appropriately.

g. Passwords must not be stored on paper, or in an electronic file, hand-held device, or browser, unless they can be stored securely [REDACTED] has been approved by the Chief Information Officer (CIO).

h. Information owners are responsible for determining who should have access to protected resources within their jurisdiction. [REDACTED]

i. Access privileges will be granted by the City of Lathrop CIO in accordance with the user's job title and will be limited only to those necessary to accomplish assigned tasks in accordance with City of Lathrop missions and business functions [REDACTED]

j. Users of privileged accounts [REDACTED]

k. Logon banners must be implemented on all systems where that feature exists to inform all users that the system is for City of Lathrop business or other approved use consistent with City of Lathrop policy, and that user activities may be monitored, and the user should have no expectation of privacy.

l. Advance approval for any remote access connection must be provided by the City of Lathrop. An assessment must be performed and documented to determine the scope and method of access, the technical and business risks involved, and the contractual, process, and technical controls required for such connection to take place [REDACTED]

m. All remote connections must be made through managed points-of-entry reviewed by the CIO. Working from a remote location must be authorized by the City of Lathrop City Manager and CIO, and best practices which ensure the appropriate protection of City of Lathrop data in remote environments must be shared with the individual prior to the individual being granted remote access [REDACTED]



Information Security Policy

Phase XII – System Security

The City of Lathrop shall maintain:

a. Systems include but are not limited to servers, platforms, networks, communications, databases, and software applications.

1. The City of Lathrop Information Services Department (ISD) must be assigned responsibility for maintenance and administration of any system deployed on behalf of the City of Lathrop.

2. Information security must be required at system inception and documented via electronic helpdesk ticket and/or change request form, as part of the decision to create or modify a system (*Appendix I: Security Awareness References. Computer Setup Check List*).

3. All systems must be developed, maintained, and decommissioned in accordance [REDACTED]

4. Each system must have a set of controls commensurate with the categorization of any information that is stored on or passes through the system (*dr*).

5. All system clocks must synchronize to a centralized reference time set to UTC (Coordinated Universal Time) which is itself synchronized to at least three synchronized time sources source [REDACTED]

6. Environments and test plans must be established to validate the system works as intended prior to deployment in production [REDACTED]

8. Formal change control procedures for all systems must be developed, implemented, and enforced. [REDACTED]

a. Databases and software [REDACTED]

1. All software written for or deployed on City of Lathrop [REDACTED]



Information Security Policy

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] or [REDACTED]

ii. sensitive data is masked or overwritten with fictional information.

4. Where technically feasible, development software and tools must not be maintained on production systems.

[REDACTED]

[REDACTED]

7. Privileged access to production systems by development staff must be restricted whenever possible.

8. Migration processes must be documented and implemented to govern the transfer of software from the development environment up through the production environment.

b. Network Systems:

1. Connections between systems must be authorized by the City of Lathrop Chief Information Officer (CIO) of all relevant City of Lathrop sites and protected by the implementation of appropriate controls.

2. All connections and their configurations must be documented, and the documentation must be reviewed by the City of Lathrop CIO annually, at a minimum, to ensure:



Information Security Policy

i. the business case for the connection is still valid and the connection is still required; and

ii. the security controls in place [REDACTED] are appropriate and functioning correctly.

3. A network architecture must be maintained that includes, at a minimum, tiered network segmentation between:

i. [REDACTED]

ii. [REDACTED] and other systems; and

iii. [REDACTED]

5. Two-factor authentication (2FA) is required for all users connecting to City of Lathrop internal systems.

6. Network Authentication is required for all devices connecting to City of Lathrop internal networks.

7. Only City of Lathrop Information Services Department (ISD) personnel may capture or monitor network traffic unless authorized by CIO for auditing purposes.

8. A risk assessment must be performed in consultation with the City of Lathrop CIO before the initiation of, or significant change to, any network technology or project, including but not limited to wireless technology.

Phase XIII – Collaborative computing Devices

The City of Lathrop Information Services Department (ISD) shall purchase and maintain:

1. Collaborative computing devices, including, for example, networked white boards, cameras, and microphones.

2. Collaborative computing devices must:

a. prohibit remote activation; and

b. provide users physically present at the devices with an explicit indication of use.

3. City of Lathrop must provide simple methods to physically disconnect collaborative computing devices. Simple methods include physically unplugging collaborative computing device from the computer or completely shutting down the computer.



Information Security Policy

Phase XIV – Vulnerability Management

The City of Lathrop shall maintain:

[REDACTED]

b. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Phase XV – Operations Security

The City of Lathrop shall maintain:

a. All systems, and the physical facilities in which they are stored, must adhere to the operating instructions, management processes, and formal incident management procedures listed within this document [REDACTED]

b. System configurations must follow CIO approved configuration standards.

c. Advance planning and preparation must be performed to ensure the availability of adequate capacity and resources. System capacity must be monitored on an ongoing basis.



Information Security Policy

d. Where City of Lathrop provides a server, application, or network service to another site, operational and management responsibilities must be coordinated by all impacted sites.

e. Host based firewalls must be installed and enabled on all City of Lathrop workstations to protect from threats and to restrict access to only that which is needed.

f. Controls must be implemented [REDACTED] across City of Lathrop systems [REDACTED]

g. [REDACTED]

i. Controls must be in place to allow only City of Lathrop approved software to run on a system and prevent execution of all other software.

j. All systems must be maintained at a vendor-supported level to ensure accuracy and integrity.

l. Any system, software, or Operating System environment which is no longer supported and cannot be patched to current versions (e.g. end of life hardware/software) must be decommissioned and removed from service.

q. Contingency plans (e.g., business continuity plans, disaster recovery plans, continuity of operations plans) [REDACTED]

2. [REDACTED]



Information Security Policy

[REDACTED]

s. Backups and restoration must be tested monthly. Separation of duties must be applied to these functions *(dr)*.

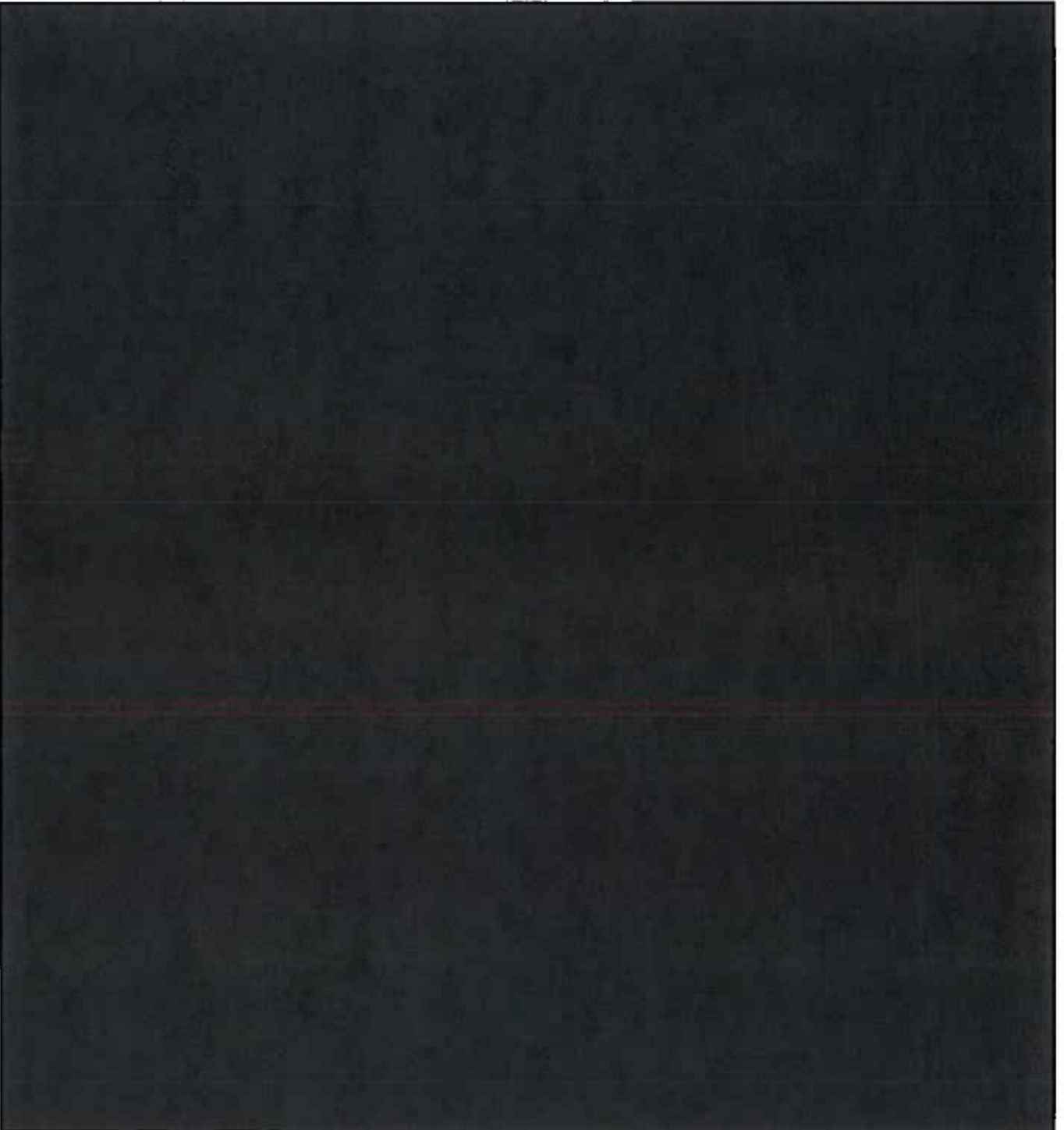
[REDACTED]



Information Security Policy

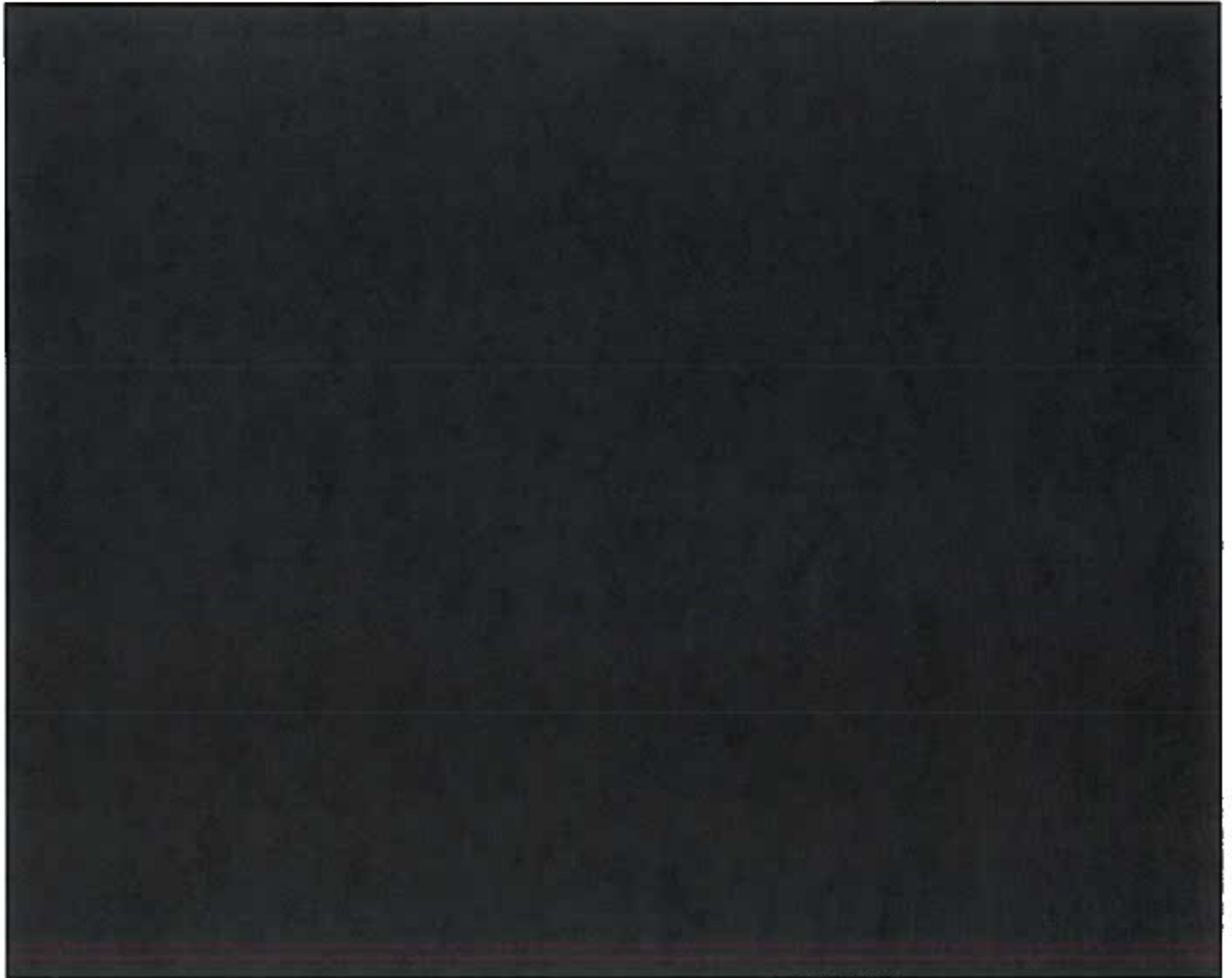
Reference

Appendix I: Security Awareness References





Information Security Policy





CITY OF LATHROP ADMINISTRATIVE REGULATION

Acceptable Use of Technology

00-17

Overview

The intention for publishing an Acceptable Use Policy is to clarify restrictions consistent with the City of Lathrop established culture of openness, trust and integrity.

We are committed to protecting City of Lathrop's employees and the City from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of City of Lathrop. These systems are to be used for business purposes in serving the interests of the City, and of our customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every City of Lathrop employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

City of Lathrop's Acceptable Use Policy helps to safeguard system assets and data, including Electronic Protected Information (EPI), against unauthorized use, disclosure, modification, damage, or loss.

Questions about this policy should be directed via e-mail to the Information Technologies Manager at helpdesk@ci.lathrop.ca.us.

Purpose

The purpose of the Acceptable Use Policy is to describe City of Lathrop's requirements for operations and is to outline the acceptable use of computer equipment at City of Lathrop. These rules are in place to protect the employees and the City. Inappropriate use exposes City of Lathrop to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to all City of Lathrop and affiliate employees, including temporary employees and employees of affiliated third-party organizations. This policy also applies to all equipment that is owned, leased, operated, or maintained by City of Lathrop.

Revision Information



Information Security Policy

When this document is updated, the reason for revision will appear here.

Policy

General Use and Ownership

1. While City of Lathrop's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the City systems remains the property of City of Lathrop. Management does not guarantee the confidentiality of information stored on any network device belonging to City of Lathrop.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use and at department head discretion.
3. The City recommends that any information that users consider sensitive or vulnerable be encrypted.
4. For security and network maintenance purposes, authorized individuals within City of Lathrop may monitor equipment, systems and network traffic at any time.
5. City of Lathrop reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by the City confidentiality guidelines to be public or confidential, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: Employee information, Payroll, customer lists, medical information, social security numbers, credit card numbers, vendor and bidder sensitive information, and lawyer/client correspondence, research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Authorized users are assigned accounts for their specific use based on their defined needs. Users are responsible for the security of their accounts.
3. Passwords are provided to enable users to keep their account secure. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords are to be changed every 90 days; user level passwords should be changed every 60 days.
4. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Windows users) when the host will be unattended.



Information Security Policy

5. Because information contained on portable computers is especially vulnerable, the computer's hard drive is encrypted to prevent access to the data in the case of the computer being lost or stolen. Password and user accounts are not to be displayed or written anywhere in the portable computer.
6. Postings by employees from a City of Lathrop email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of City of Lathrop, unless posting is in the course of business duties.
7. All hosts used by the employee that are connected to the City of Lathrop Internet/Intranet/Extranet, whether owned by the employee or City of Lathrop, shall be continually executing approved virus-scanning software with a current virus database.
8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

Unacceptable Use

The following activities are, in general, prohibited. Information Technologies Staff may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., there may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of City of Lathrop authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing City of Lathrop owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by City of Lathrop .
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which City of Lathrop or the end user does not have an active license is strictly prohibited.



Information Security Policy

3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a City of Lathrop computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any City of Lathrop account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to the IT Department is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, City of Lathrop employees to parties outside City of Lathrop.
16. Sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
17. Any form of harassment via email, paging, whether through language, frequency, or size of messages.



Information Security Policy

18. Unauthorized use, or forging, of email header information.
19. Solicitation of email from any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
20. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
21. Use of unsolicited email originating from within City of Lathrop 's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by City of Lathrop or connected via City of Lathrop 's network.
22. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
23. Video, audio and /or any type of internet streaming not for business purposes.

Electronic Data Access

Only Department Heads or the Information Systems Manager with the approval of the City Manager can authorize the reading of electronic media information, which includes, but is not limited to, e-mail and voicemail messages, for employees under their supervision. For City Manager would have to be approved by at least three City Council Members. The City will also respond to legal processes and fulfill any obligations to third parties with the approval of the City Attorney.

Privacy

1. All information created by employees or use by employees is not confidential or private. All of the City's electronic media and information relating to these electronic media are City property information and records are also subject to disclosure to the public. Although employees have passwords that restrict access to their computers, the City reserves the right to and routinely does access this information.
2. It should be noted that even though information or files may have been deleted from electronic media, it does not mean that they have been permanently erased from the systems. This includes e-mail and messages stored on external electronic media systems such as Microsoft Hotmail or Instant Messaging that may have been viewed, read, printed, or stored (permanently or temporarily), on City equipment.
3. In addition to the foregoing provisions, employees should be aware that certain kinds of electronic media information may be subject to record retention requirements employees may not delete any such protected records, either as "public records" or pursuant to discovery in litigation.



Information Security Policy

Wireless Network Equipment

1. Written permission must be obtained from the IT Manager and authorized before any wireless network device can be connected to City of Lathrop networks.
2. Deployment of ANY wireless access points without IT Manager's permission is strictly prohibited.
3. All wireless network devices connecting to City networks must be configured by the IT Department. At no time should laptop computers, handheld computers or PDAs (Personal Digital Assistant), or other wireless devices be connected to the City's internal network without the prior approval of the IT Department. The exception would be any designated public wireless access point or public hotspot deployed by the City of Lathrop.

Enforcement

Disciplinary actions for City staff are defined in the City's Personnel Rules & Regulations Manual.

Definitions

Term	Definition
Spam	Unauthorized and/or unsolicited electronic mass mailings
EPI	Electronic Protected Information – Examples are; Employee information, Payroll information, customer lists, medical information, social security numbers, credit card numbers, etc.



Information Security Policy

Vendor Remote Log-In Questionnaire



Information Systems Department

390 Towne Centre Dr. – Lathrop, CA 95330
Phone (209)941-74300 – Fax (209) 941-7219
www.ci.lathrop.ca.us

Remote Log-In Questionnaire

[Redacted content]

Requestor Signature

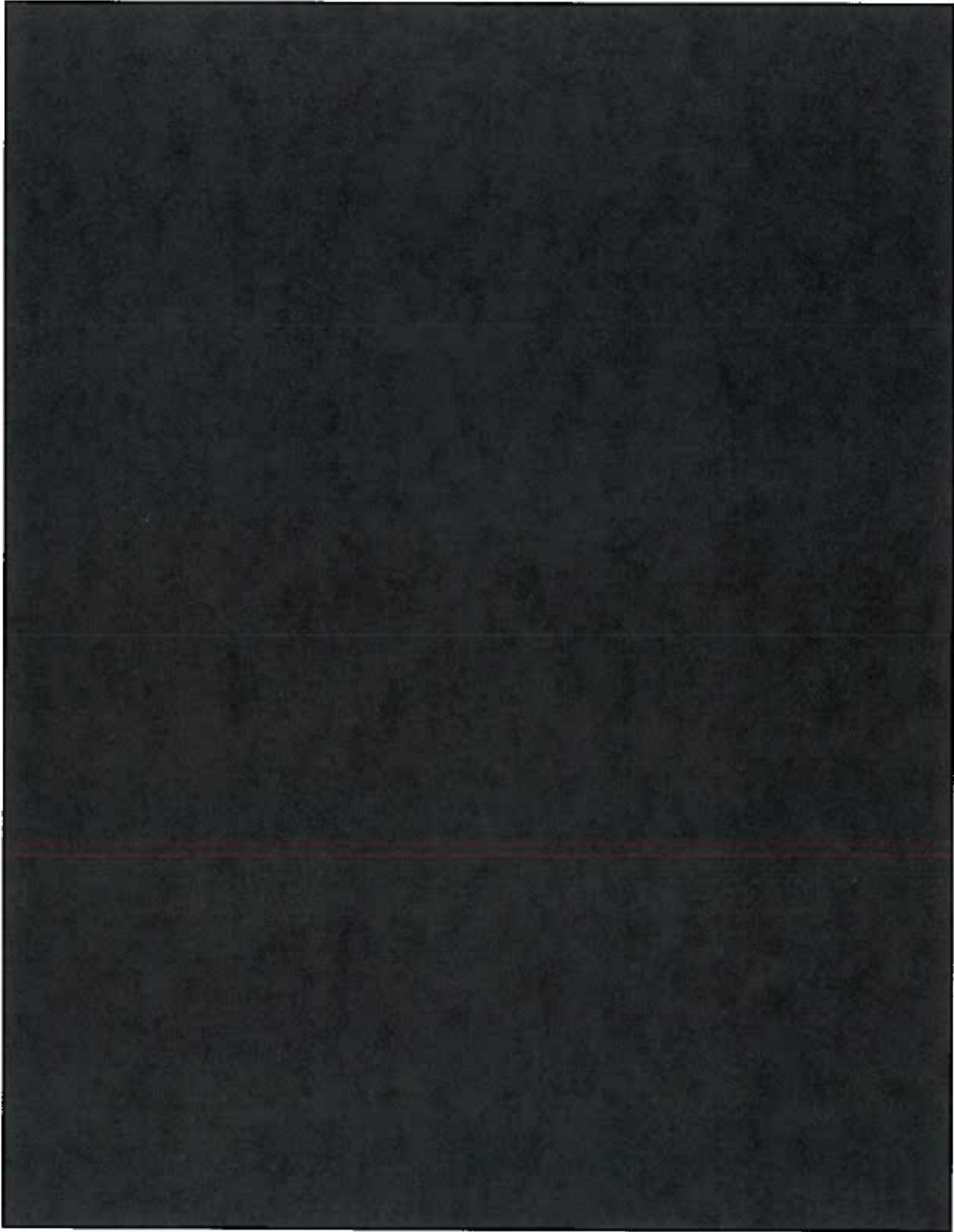
Date

City of Lathrop CIO Signature

Date



Information Security Policy





Information Security Policy

Contact Information

Listed personnel that should be contacted in the event of data loss incidents.

Updated March 2023

Name	Title	Role	Contact Information	Escalation (1-3)*
	Information Security Risk Coordinator	CSIST Commander		
	Asset Manager	CSIST Commander		
	Infrastructure Manager	CSIST Manager		
	CIO	CIO		
	Communications Manager	CSIST member		
	Legal	CSIST member		
	Risk Manager	CSIST member		
	HR Representative	CSIST member		
	Physical Security Representative	CSIST member		
	3 rd Party Support			
FBI				
	Regulatory/Government Reporting Body			

*Escalation level determines order in which notification should occur in the event of a data loss incident:

1. Notify first, required on all incidents
2. Required on all moderate or high-severity incidents
3. Involve as needed



Information Security Policy

Information Security Team Members

Updated March 2023

No.	CSIRT Member	Role
1		CSIST Commander
2		Network Subject Matter Expert
3		Network Subject Matter Expert
4		Senior IT Staff
5		Systems Engineer
6		Recorder
7		Recorder



Executive Summary

A Cyber Security Incident is defined as an event that breaches or violates the Confidentiality, Integrity or Availability (CIA) of City of Lathrop Information systems. Failure to act quickly and efficiently in accordance with best practices and relevant requirements can result in a loss of functionality and reputation damage, but also potential steep financial penalties. To avoid the worst fallout of a cyber-incident, it's vital that the components of your incident response plan (IRP) are built with consideration of industry guidelines, cyber legislation, and your organizations unique risk profile.

Incident Response Plan

An Incident Response plan is important to address issues that were not stopped by preventative systems and procedures. No system can be 100% secure. Reasonable steps and best practices such as Information Security Policies, Encryption guidelines, Security Awareness training and other measures are implemented to prevent incidents from occurring. However, when an attacker is successful in penetrating the layers of security, a plan of action needs to be predefined to ensure efficient containment and remediation of the event.

This policy provides the framework to addresses the seven steps necessary to minimize the negative effects of a security breach. These steps are as follows:

Preparation: Identify risks and establish roles and responsibilities to address those risks.

Identification and Assessment: Training and evaluation for defining and detecting a threat and to determine if there is a need to activate the plan.

Containment and Intelligence: The containment section will outline the strategies for limiting the scope of the incident.

Eradication: The procedures for removing the threat from all affected systems through to the recovery of all affected systems.

Recovery: Implementation of restore functions of the Data Backup and Retention Policy to recover lost or damaged information as well as replacement or reconfiguration of damaged systems.

Lessons Learned: Once the incident is resolved it must be determined how the breach occurred, how to prevent similar incidents and preparation of a plan to address necessary changes.

Introduction

The City of Lathrop Incident Response Plan has been developed to provide guidance to the handling of information security incidents that adversely affect City of Lathrop Information Resources. The City of Lathrop Incident Response Plan applies to any person charged by the City of Lathrop Incident Response Commander with a response to information security related incidents.

The purpose of the Incident Response Plan is to allow the City of Lathrop to respond quickly and appropriately to information security incidents.



City of Lathrop Incident Response Plan

Event Definition

Any abnormal observable occurrence in system, network, environment, process, workflow, or personnel. Events may or may not be negative in nature.

Adverse Events Definition

Events with a negative consequence. This plan only applies to adverse events that are computer security related, not events caused by natural disasters, power failures, etc. which are covered in the Business Continuity-Disaster Recovery Plan.

Incident Definition

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices that jeopardizes the confidentiality, integrity, or availability of information resources or operations. A security incident may have one or more of the following characteristics:

- A. Violation of an explicit or implied City of Lathrop security policy
- B. Attempts to gain unauthorized access to a City of Lathrop Information Resource
- C. Denial of service to a City of Lathrop Information Resource
- D. Unauthorized use of City of Lathrop Information Resources
- E. Unauthorized modification of City of Lathrop information
- F. Loss of City of Lathrop Confidential or Protected information