CITY MANAGER'S REPORT
APRIL 10, 2023 CITY COUNCIL REGULAR MEETING

ITEM 4.20

ITEM: **GRAND JURY REPORT RESPONSE UPDATE**

RECOMMENDATION: **Direct the City Attorney to Submit a Letter to the Presiding Judge of the San Joaquin County Superior Court Responding with an Update to the Findings and Recommendations of the Grand Jury Report On Cybersecurity.**

SUMMARY

On September 12, 2022 at its regularly scheduled City Council meeting, the City Council accepted the 2021/2022 San Joaquin County Grand Jury Final Report for Case No. 0321 regarding cyber security ("Attachment A") and directed the City Attorney to send a response letter ("Attachment B"). Within Findings and Recommendations 3.3 and 3.4, The Grand Jury recommended the City develop, adopt and implement a formal, written Business Continuity Plan and develop, adopt and implement formal, written, internal policies and procedures for potential ransomware attacks.

The City agreed with Findings and Recommendations 3.3 and 3.4, and instructed staff to draft written cyber security policies and procedures.

BACKGROUND

On September 12, 2022 at its regularly scheduled City Council meeting, the City Council accepted the 2021/2022 San Joaquin County Grand Jury Final Report for Case No. 0321 regarding cyber security and directed the City Attorney to send a response letter. Within Findings and Recommendations 3.3 and 3.4, The Grand Jury recommended the City develop, adopt and implement a formal, written Business Continuity Plan and develop, adopt and implement formal, written, internal policies and procedures for potential ransomware attacks.

City staff, with the assistance of hired consultants and the City's insurer, drafted Information Systems Department procedures and provided drafts of those policies regarding cyber security to the Grand Jury on March 28, 2023 as further response to the Final Report for Case No. 0321 Findings and Recommendations 3.3 and 3.4. The Grand Jury provided the requested edits or changes. Therefore, to finalize the City's response, staff requests City Council approval of the following updated responses:

> **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.

Proposed 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.

Proposed 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.

RECOMMENDATION:

Staff recommends City Council consider approval of the City's proposed updated responses to the Grand Jury and direct the City Attorney to submit responses to the Presiding Judge of the San Joaquin County Superior Court to the findings and the recommendations outlined in the Grand Jury Final Report for Case No. 0321.

FISCAL IMPACT:

None, except for staff time to prepare this report.

ATTACHMENTS:

A. Grand Jury Final Report, Case No. 0321
B. Letter to San Joaquin County Superior Court Presiding Judge in response to Grand Jury Final Report Case #0321 dated September 13, 2022.
C. Draft Letter to San Joaquin County Superior Court Presiding Judge in follow-up response to Grand Jury Final Report Case #0321
D. City of Lathrop Draft Incident Response Plan Executive Summary and Introduction
E. City of Lathrop Draft Information Security Policy
F. City of Lathrop Draft Business Continuity-Disaster Recovery Plan

APPROVALS:

Tony Fernandes
Director of Information Systems

4-4-2023
Date

Salvador Navarrete
City Attorney

4/5/2023
Date

Stephen J. Salvatore
City Manager

4·6·23
Date

Attachment A

2021–2022 San Joaquin County Grand Jury

San Joaquin County and Its Seven Cities:
Cybersecurity: Local Defense Against a Global Threat
Case #0321

Summary

We hear reports on a daily basis of cyberattacks occurring around the world. These attacks are becoming increasingly sophisticated, disruptive and expensive. Attacks on government agencies can disrupt essential services, crippling communities. Agencies small and large are equally vulnerable. There is an ever-growing demand for stolen data in an underground market. Compromise of information has proven to be a serious threat on the cyber battleground, both domestically and internationally. Bad actors hack intelligence, media and essential service systems. Other disasters such as floods, fires, storms or prolonged power outages can interrupt essential services if providers' information systems are not adequately secure. According to one expert witness interviewed by the 2021-2022 Grand Jury, "World War III will be fought in cyberspace, not on the battlefield."

Grand Jury members are not technical experts but sought to understand the cybersecurity landscape and local governments' management of their cybersecurity risks and vulnerabilities. In this investigation of information security of San Joaquin County and its seven cities, the 2021-2022 Grand Jury made a "point in time" assessment of each entity's Information Systems Department (ISD), focusing primarily on cybersecurity. The Grand Jury considered nine elements of any ISD and, through research of relevant literature and input from industry experts, established an expected standard for each of those elements. The Grand Jury then evaluated each of the agencies with respect to those expectations.

The Grand Jury concluded that San Joaquin County (SJC) has mature and robust security policies and systems. The County's security architecture provided a model in evaluating each city's systems. The Grand Jury determined that Escalon, Lodi and Stockton met a lay person's expectations for cybersecurity but were lacking either a formal Business Continuity Plan (BCP) or Disaster

Preparedness Plan (DPP). Lathrop, Manteca and Tracy were found to have adequate security systems in place but lack documented plans for both Business Continuity and Disaster Preparedness. Ripon was found to-need improvement in meeting several of the Grand Jury's expectations, with lack of personnel being their greatest challenge.

The Grand Jury recommends that the County and affected cities:

- develop, adopt and implement a Business Continuity Plan;
- develop, adopt and implement an IT Disaster Preparedness Plan;
- remedy specific cybersecurity risks found in this investigation; and
- the City of Ripon undergo a data system security review by an expert third party to assess the City's IT systems and protocols.

The Grand Jury recognizes that cybersecurity is a dynamic process, a continually moving target which needs constant monitoring and updating.

Glossary

- **Access:** The ability and means to communicate with or otherwise interact with a system; to use system resources to manage information; to gain knowledge of the information the system contains; to control system components and functions.
- **Actor, bad actor, threat actor or attacker:** An individual, group, organization or government that attempts or executes an attack.
- **Attack:** An intentional attempt to gain unauthorized access to system services, resources or information; an attempt to compromise system integrity.
- **Authentication:** The process of verifying the identity or other attributes of an entity (user, process or device).
- **Authorization:** A process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource.
- **BCP:** Business Continuity Plan. A document that sets forth procedures for the continued performance of core capabilities, critical operations and user services during any disruption or potential disruption.
- **CCISDA:** California County Information Services Directors Association. This is the official organization of the county IT directors and chief information officers throughout the state of California. CCISDA represents all 58 California counties in the area of information technology in county government.
- **CIO:** Chief Information Officer.
- **Computer Aided Dispatch Systems:** Used by dispatchers, call-takers, and 911 operators to prioritize and record incident calls, identify the status and locations of responders in the field and effectively dispatch responders.
- **Confidentiality:** A property of information that is not disclosed to users, processes or devices unless they have been authorized to access the information.
- **Cyber event or incident:** An occurrence that actually or potentially results in adverse consequences to an information system or the information that the system processes, stores or transmits and that may require a response action to mitigate the consequences. An occurrence that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies.

- **Cybersecurity**: The activity, process, ability, capability or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use, modification or exploitation.
- **DPP**: Disaster Preparedness Plan. A document that sets forth policies and procedures for restoration of information systems after a critical incident or event from any source. The plan addresses interim restoration of information operations in the short and medium term and full restoration of all capabilities in the longer term.
- **Data integrity**: The property that data is complete, intact and trusted and has not been modified or destroyed in an unauthorized or accidental manner.
- **Data security policy**: A rule or set of rules that governs the acceptable use of an organization's information and services to a level of acceptable risk and the means for protecting the organization's information assets.
- **Encryption**: The process of converting data into a form that cannot be easily understood by unauthorized people or agents.
- **Firewall**: A capability to limit network traffic between networks and/or information systems. A hardware/software device, or a software program, that limits network traffic according to a set of rules of what access is and is not allowed or authorized.
- **Hacker**: An unauthorized user who attempts to or gains access to an information system.
- **ISD**: Information Systems Department.
- **IT**: Information Technology.
- **KnowB4**: A proprietary security awareness training platform. KnowB4 is used by agencies for simulated phishing activities and other email compromise tests, as well as for other IT security training needs.
- **Malware**: Software that compromises the operation of a system by performing an unauthorized function or process.
- **Mobile device management tool**: A security software tool designed to help organizations secure, manage and monitor mobile devices such as smartphones and tablets.
- **Multi-factor authentication**: An electronic authentication mechanism in which a user is granted access to an application only after presenting two or more pieces of evidence (factors or keys only the authentic user knows or possesses).
- **Multi-layer security access**: Multi-layer security refers to a system that uses numerous components to shield the IT infrastructure. It is a defense mechanism that mitigates, delays or prevents threats.
- **Network or cyber infrastructure**: The information and communication systems and services composed of all hardware and software that process, store and communicate information; any combination of all these elements.
- **Next-generation systems**: Security systems consisting of both firewall and intrusion prevention systems built in, rather than as add-ons, along with the features of basic firewalls.
- **Phishing**: A digital form of social engineering to deceive individuals into providing sensitive information.
- **Phishing test**: A security training exercise designed to test users' vulnerability and reinforce vigilance.
- **Presidential Executive Order 14028**: "Improving the Nation's Cybersecurity" (issued May 12, 2021) requires agencies to enhance their cybersecurity system integrity.

- **Ransomware:** A type of malicious software designed to block access to a computer system until a sum of money is paid.
- **Ransomware attack response plan:** A set of predetermined and documented procedures to detect and respond to a cyber incident involving demand for ransom for recovery and restoration of data or systems.
- **Records Management System:** The management of records for an organization throughout the records' life cycle.
- **Redundancy:** Additional or alternative systems, sub-systems, assets or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, asset or process. Typically applied to power supplies and data backup systems.
- **Vulnerability:** A characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard.

  Wi-Fi network: A family of wireless network protocols used for local area networking of devices and internet access, allowing nearby digital devices to exchange data by radio waves.

Background

The 2008-2009 San Joaquin County Grand Jury reported on information technology security, finding that several County departments and two of the seven cities in the county met expectations for Information Technology (IT) security, while some County departments and five cities did not. Recommendations were made and generally accepted in agency responses. In terms of technology, 2008-2009 was at least a generation ago. Government agencies use and store vast amounts of sensitive data on their residents and their employees, including personal identification data, financial data, health data and legal data. Additionally, these agencies provide services essential to our day-to-day lives, including public safety (police and fire), public works, health services, water services and community development. The Grand Jury recognizes that we are lay people, hardly experts, in the field of IT. It was the intent of the 2021-2022 Grand Jury to examine how the county and city governments within San Joaquin County are exercising due diligence to protect information, defend against future cyberattacks, maintain current disaster plans and provide on-going training to employees in these matters.

Reason for Investigation

As stated in Presidential Executive Order 14028, "...the prevention, detection, assessment and remediation of cyber incidents is a top priority and essential to national economic security."

San Joaquin County has experienced ransomware and cybersecurity attacks firsthand. School districts, municipalities and county agencies have been victimized in recent years. Given the rise in complexity of IT, the current sophistication of cybercrime, and the essential nature of government services provided, the 2021-2022 Grand Jury undertook an investigation into the current state of security and disaster preparedness of the IT systems of San Joaquin County and the seven incorporated cities within the county.

Method of Investigation

The 2021-2022 Grand Jury surveyed six San Joaquin County IT department heads and the City Manager or City Administrator of each of the seven cities in the county; each responded to the survey. Subsequently, an agency IT department head or staff member, an IT consultant or a city administrator was interviewed to clarify responses and to provide additional material when applicable. The Grand Jury also interviewed independent cybersecurity experts. The expert witnesses have collectively more than 50 years' experience at diverse levels of government ranging from county to state to national information systems and cybersecurity. IT executives from one school district were also interviewed. For this investigation, the Grand Jury interviewed 16 individuals and attended cybersecurity presentations.

The Grand Jury also reviewed numerous websites and newspaper and magazine articles relevant to this investigation. Additionally, the Grand Jury reviewed documents provided, including network diagrams, ransomware insurance policies and other items.

Materials Reviewed

- 2021-2022 San Joaquin County Grand Jury surveys
- Biden, Joseph. *Executive Order on Improving the Nation's Cybersecurity*. 12 May 2021. Executive Order#14028
- *California Joint Cyber Incident Response Guide*. California Office of Emergency Services Cyber Security Integration Center, 2 Aug. 2021
- *Cyber Atack Preparedness in Contra Costa County*. Contra Costa County Civil Grand Jury, 2021. Report 2104
- *Digital Services and Innovation Strategy*. San Joaquin County, 19 Nov. 2020
- *How to Develop a Ransomware Remediation Plan*. Rubrik, 2021
- *Information Technology Security*. 2018-2019 Santa Barbara County Grand Jury, 2019
- *Information Technology Security: Cities and San Joaquin County*. 2008/2009 San Joaquin County Grand Jury, 2009. Report No.03-08
- *Ransomware Defense for Dummies--2nd Edition*. 2nd ed., Cisco Umbrella, 2021

Websites Visited

- Cybersecurity & Infrastructure Security Agency. "CYBERSECURITY | CISA." *Cisa.gov*, Cybersecurity and Infrastructure Security Agency, 2019, www.cisa.gov/cybersecurity. Accessed 6 May 2022.
- Federal Trade Commission, and Alvaro Puig. "Cybersecurity Advice to Protect Your Connected Devices and Accounts." *Sjgov.org*, 24 Mar. 2022, www.sjgov.org/department/da/consumer-alerts/consumer-alerts/2022/03/24/cybersecurity-advice-to-protect-your-connected-devices-and-accounts. Accessed 6 May 2022.
- Kuykendall, By Kristal. "Cybersecurity Experts Call for More Transparency and Immediate Resources for Schools -." *The Journal*, 17 Mar. 2022, thejournal.com/Articles/2022/03/17/Cybersecurity-Experts-Call-For-More-Transparency-and-Immediate-Resources-for-Schools.aspx?Page=1. Accessed 6 May 2022.

- Marcum Accounts Advisors. "What Is a SOC 2?" *The SSAE 18 Reporting Standard - SOC 1 - SOC 2 - SOC 3 (Formerly SSAE 16)*, 8 Jan. 2022, www.ssae-16.com/faq/what-is-a-soc-2/. Accessed 30 Apr. 2022.
- National Institute for Cybersecurity Careers and Studies. "Cybersecurity Glossary | National Initiative for Cybersecurity Careers and Studies." *Niccs.cisa.gov*, niccs.cisa.gov/about-niccs/cybersecurity-glossary. Accessed 6 May 2022.
- Unisys. "Cyber Attacks--What You Need to Know." *Unisys*, 2022, www.unisys.com. Accessed 6 May 2022.

Discussions, Findings and Recommendations

General Discussion

The Grand Jury recognizes cybersecurity is an extremely complicated topic. Specialized knowledge, experience and expertise are required for a deep understanding of what is necessary for adequate policies, systems and architecture. Lacking such specialized knowledge, the Grand Jury researched numerous sources, including recognized experts in this field to determine the following elements of any ISD and to define the following expectations for adequate cybersecurity in today's environment.

Expectations

- **Organization:** Each organization should have a detailed Organization Chart demonstrating the structure of its independent IT department. Cities lacking an independent IT department should have a chart showing where IT resides in their overall structure.
- **Network Diagram:** Each organization should have a detailed network diagram indicating the relationships between all IT architectural elements. Best-practice guidelines suggest that this diagram be confidential.
- **Data Confidentiality:** Each organization should have an organization-wide policy determining data confidentiality and access control. Policy for data access should be clearly defined and desk-specific or station-specific.
- **Data Security:** Each organization should have next-generation systems and controls to ensure both physical and cyber security for all IT assets. Next-generation firewalls and endpoint management systems provide protection against ever-evolving means of cyberattack. Data should be protected with daily or continuous backup and archival systems. Backups should be protected against corruption, external encryption and/or destruction. Agencies should require multi-factor authentication for access to network systems.
- **Business Continuity Plan (BCP):** Each organization should have a detailed, current, comprehensive plan for restoring services in the event of disruption from any source.
- **Disaster Preparedness Plan (DPP):** Each organization should have a formal, detailed plan to prepare for various possible IT disruptions. This plan should be tested frequently and updated regularly.
- **Ransomware Policy:** Each organization should have an internal (confidential) documented policy for agency response to a ransomware attack.

- **Cyber Event Insurance:** Each organization should have insurance coverage to help offset economic losses from cyber events.
- **Ongoing Employee Training:** Each organization should provide rigorous, frequent training and ongoing testing of all employees as an integral part of its cybersecurity profile.

Survey Results:

The table below indicates whether an agency met (M), did not meet (NM) or was in the process of meeting (IP) the nine defined expectations.

	Org Chart	Network Diagram	Data Confidentiality	Data Security	BCP	DPP	Ransomware Policy	Cyber Insurance	Training
SJC	M	M	M	M	M	M	NM	M	M
Escalon	M	M	M	M	NM	M	M	M	M
Lathrop	M	M	M	M	NM	M	NM	NM	M
Lodi	M	M	M	M	IP	M	M	M	M
Manteca	M	M	M	M	M	M	IP	IP	M
Ripon	M	M	M	M	NM	NM	NM	M	M
Stockton	M	M	M	M	M	M	NM	M	M
Tracy	M	M	M	M	IP	IP	NM	M	M

1.0 San Joaquin County–Discussion

In November 2020, San Joaquin County released a three-year (2020-2023) strategic plan for ensuring continuing security, efficacy, cost-effectiveness and best-service outcomes to all end-users of County services and systems. The plan document "San Joaquin County Digital Services and Innovation Strategy" established goals for County digital service systems. These goals—Modernizing and Leveraging Our Technology Environment—address objectives for a security posture:

1. Acquire and implement cybersecurity technology to enable SJC to develop industry-leading capabilities to help mitigate and address cybersecurity risk.
2. Develop and mature security governance and processes to meet or exceed industry standards, enhance security enforcement partnerships, and strengthen County practices.
3. Develop a robust security training program for the County workforce, including enhanced training and development for the security workforce.

Excerpt from "San Joaquin County Digital Services and Innovation Strategy," November 19, 2020 (page 6)

San Joaquin County has met these objectives and continues to update and enhance these processes as the cybersecurity landscape continues to evolve.

San Joaquin County ISD oversees all County departments, making it one of the largest county ISDs in California. San Joaquin County ISD is an active participant in the California County Information Systems Department Association (CCISDA). This association provides opportunities for counties to share information and experiences and offers guidance, such as standards for best-practice policies. Several large and specialized departments within the County have their own IT departments and department chiefs who report to the County's Chief Information Officer. Additionally, SJC has a dedicated Information Security Officer. All these IT executives form a cybersecurity governance committee which meets monthly, with subgroups meeting more frequently as needed.
County ISD and Human Resource Departments conduct frequent and on-going employee training and testing using proprietary software. In addition to these County departments, several Independent Special Districts in SJC use County IT services through various memoranda of understanding.
The only element of the defined expectations not met by SJC is having an internal documented policy for response to a ransomware attack.
San Joaquin County is a model agency in the realm of information technology and maintenance of cybersecurity.

Findings

F1.1 San Joaquin County does not have a formal internal policy concerning payments or procedures in ransomware attacks. This absence of policy could cause confusion, delay and greater loss of security in the event of such an attack.

F1.2 San Joaquin County has an exemplary profile regarding cybersecurity and should serve as a model for other government agencies within San Joaquin County.

Recommendations

R1.1 By November 1, 2022, the San Joaquin County Board of Supervisors, in conjunction with San Joaquin County ISD, develop, adopt and implement a formal internal policy and procedure for response to a ransomware attack.

2.0 City of Escalon–Discussion

The City of Escalon does not have an independent IT department but has a contract agreement with Mid Valley IT to provide all IT services. In the City organization, IT functions report to the Finance and HR Directors. Each employee is given a level of access according to assigned responsibilities within their department. All employees receive information security training specific to their responsibilities as well as general security awareness training. The IT consultant employs an aggressive multi-layered approach to mitigate security threats through software and hardware protection measures. Critical or confidential data is stored in multiple cloud-based locations and systems employing numerous safeguards, including use of multi-factor authentication for access.

IT functions are protected with a standby generator and redundant backups in case of a system failure. The generator is tested periodically for functionality.

The City of Escalon met all but one of the expectations for adequate cybersecurity. Escalon is by far the smallest city in San Joaquin County, but by using a contracted IT service provider, Escalon is meeting its cybersecurity needs. The City of Escalon does not have a documented Business Continuity Plan.

Findings

F2.1 The City of Escalon does not have a documented Business Continuity Plan, leaving the City relatively unprepared to restore essential services in a disruptive event.

Recommendations

R2.1 By January 1, 2023, the Escalon City Council, in conjunction with Mid Valley IT, develop, adopt and implement a Business Continuity Plan.

3.0 City of Lathrop–Discussion

The City of Lathrop met six of the expectations for the nine elements considered in this investigation. Lathrop's IT organization includes a Director of Information Technology at the cabinet leadership level, a policy strongly recommended by an IT expert for maximum IT security. Including the Director of IT in frequent, regular meetings with other department heads allows effective communication of IT security needs to all City departments.

Expectations for data confidentiality and data security were met. However, use of multi-factor authentication for system access was not universal at the time of this investigation, leaving Lathrop at higher risk of attack. Lathrop provides an unsecured public Wi-Fi network, separate from the City's secure business network and accessible to any user. Hackers or other bad actors could take advantage of the unsecured network, possibly resulting in compromise of log-in credentials from that network and possibly exposing the City to costly liability suits. Lathrop was in the process of developing and approving a BCP and DPP plan at the time of this investigation. Similarly, the City was updating an internal policy for response to a ransomware attack. At the time of this investigation, Lathrop lacked insurance against losses incurred in a cybersecurity incident.

Findings

F3.1 The City of Lathrop does not employ multi-factor authentication universally, leaving City systems more vulnerable to the activities of bad actors.

F3.2 The City of Lathrop provides an unsecured public Wi-Fi network. Misuse of this unsecured network could expose the City to liability risks.

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.

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.

F3.5 The City of Lathrop does not have an insurance policy covering financial losses from a cyberattack, possibly exposing City financial resources.

Recommendations

R3.1 By November 1, 2022, the Lathrop City Council, in conjunction with the City's IT department, develop, adopt and implement a procedure for universal multi-factor authentication for access to City data.

R3.2 By November 1, 2022, the Lathrop City Council, in conjunction with the City's IT department, provide a secure public Wi-Fi network.

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.

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.

R3.5 By January 1, 2023, the Lathrop City Council, in conjunction with the City's IT department, obtain an insurance policy to mitigate fiscal impact resulting from cyberattack or other critical information system loss.

4.0 City of Lodi–Discussion

The City of Lodi has a large IT division, responsible for all IT functions of the City. The division is responsible for the integrity of the City's cyber infrastructure, maintenance and support of all hardware and software, and assuring secure access to all network resources. Lodi fell victim to a ransom attack in April 2019. That unfortunate event caused the City to change its management of cybersecurity, significantly elevating the importance of vigilance by all City staff. Lodi has implemented a robust cyber awareness training program for all City employees, incorporating education in tactics used by bad actors both inside and outside the City's network. Monthly training is followed by testing in topics covered. Citywide campaigns occur quarterly to test employee response to phishing and other email-based attacks. The IT division head reports directly to the Deputy City Manager and meets regularly with all City department heads. The City of Lodi met all expectations for cybersecurity except for having a completed, up-to-date Business Continuity Plan. The City has contracted a business consulting firm to create a BCP, projected to be completed and implemented by the end of June 2022.

Findings

F4.1 The City of Lodi does not have an approved Business Continuity Plan, rendering the City relatively unprepared to restore essential services in a disruptive event.

F4.2 The City of Lodi has implemented an excellent cyber awareness training program for all employees minimizing risk to damage from cyberattack.

Recommendations

R4.1 By January 1, 2023, the Lodi City Council, in conjunction with the City's IT division, develop, adopt and implement a Business Continuity Plan.

5.0 City of Manteca–Discussion

The City of Manteca met seven of the nine expectations considered in this investigation. Manteca's Information Technology department is independent in the City's organization. The department director reports directly to the City Manager and meets weekly with other City department heads. User level of access is determined by position, background and other departmental factors. Employees are trained on a regular basis. The training is mandatory for all employees. Hard drives are encrypted, and a Mobile Device Management tool is used for tablets, laptops and phones.

Manteca's ISD is currently updating its Information Technology Security Policy. This comprehensive policy has not been updated since 2010. Manteca's Department of Information Technology and Innovation is collaborating with City administration and the City Attorney to update all policies relating to information technology security. Similarly, the City is in the process of bringing both hardware and software systems up to next-generation standards with new firewall, malware, user access, backup systems and applications in place. Employee training is executed through KnowB4, an industry-standard cybersecurity training program which includes phishing and other email compromise testing.

Regarding firewalls and switches, roughly 60% still operate off single rather than dual or redundant power supplies. Over the next five years, the City is phasing out older devices as they reach end-of-life.

Findings

F5.1 The City of Manteca has an Information Technology Security Policy which has not been updated since 2010, leaving the City relatively unprepared for a cyber event.

F5.2 The City of Manteca lacks a policy and procedure for ransomware attacks. This absence of policy could cause confusion, delay, and greater loss of security in the event of such an attack.

F5.3 The City of Manteca has a significant number of security devices with single power supplies. This lack of redundant power presents vulnerability in major or prolonged power outages.

Recommendations

R5.1 By January 1, 2023, the Manteca City Council, in conjunction with the City's ISD, develop, approve and implement an updated Information Technology Security Policy.

R5.2 By January 1, 2023, the Manteca City Council, in conjunction with the City's ISD, develop, approve and implement a confidential policy and procedure for response to a ransomware attack.

R5.3 By March 1, 2023, the Manteca City Council, in conjunction with the City's ISD, develop, approve and adopt an updated timeline to replace single-powered units with dual-powered or redundant-powered units in their network architecture.

6.0 City of Ripon–Discussion

The City of Ripon has experienced turnover and vacancies in the IT Department in the past year. The Director of IT resigned in early 2021. Subsequently, another IT Director was hired but resigned within three months. The City has contracted with a former IT employee as a temporary IT Director and is currently updating the job description for a permanent director of the IT functions.

The City's organization chart does not include an IT department or department head. The only IT position shown is within the Police Department.

Data confidentiality is maintained through a three-tiered access structure. Management supervisors for each City department determine who has access to appropriate information. Sensitive data is held within a Computer Aided Dispatch Program or a Records Management System within the IT division of the Ripon Police Department. The sensitivity of data with all other City departments is determined by supervisors.

Findings

F6.1 It is unclear in the City of Ripon's Organization Chart where responsibilities for IT and IT security lie, creating confusion over who is responsible to act in a disruptive event.

F6.2 The City of Ripon has a rudimentary network diagram outlining the City's router and firewall relationship with networks used, but the diagram lacks detail, leaving uncertainty about data security.

F6.3 Although the City of Ripon met expectations in the areas of data confidentiality and security, lack of IT staff and leadership leaves these areas vulnerable to cyberattack.

F6.4 The City of Ripon lacks a Business Continuity Plan, rendering the City relatively unprepared to restore essential services in a disruptive event.

F6.5 The City of Ripon does not have a Disaster Preparedness Plan, leaving the City at risk for significant delay and cost to restore IT systems in the event of a disaster.

F6.6 The City of Ripon does not have a formal policy or procedure to address ransomware attacks. This absence of policy could cause confusion, delay and greater loss of security in the event of an attack.

Recommendations

R6.1 By January 1, 2023, the Ripon City Council develop and make public an updated City Organization chart showing details of the City's IT functions, including all IT positions.

R6.2 By January 1, 2023, the Ripon City Council develop and adopt a detailed Network Diagram to decrease security vulnerabilities.

R6.3 By January 1, 2023, the Ripon City Council obtain a third-party security review of the City's IT department assets, positions, and policies and an evaluation of data confidentiality, security systems and protocols.

R6.4 By January 1, 2023, the Ripon City Council develop, adopt and implement a formal Business Continuity Plan.

R6.5 By January 1, 2023, the Ripon City Council develop, adopt and implement a formal Disaster Preparedness Plan for IT functions.

R6.6 By January 1, 2023, the Ripon City Council develop, adopt and implement a formal internal policy and procedure for response to a ransomware attack.

7.0 City of Stockton–Discussion

The City of Stockton has a large IT department that oversees IT functions for all the City's other departments. Data confidentiality and user access are determined departmentally, following uniform standards. Information is protected by many safeguards aiming not only to minimize risk of penetration but also to detect any breach that might occur. Stockton has both a BCP and a DPP. Stockton is one of very few cities having license to use a cybersecurity tool integrating the City with the State of California's Office of Emergency Services. Stockton's IT Director meets weekly with other department heads, updating them on all matters related to cybersecurity.

Stockton met each of the cybersecurity expectations except for the presence of a documented internal policy and procedure for response to a ransomware attack. However, the City does have a Cybersecurity Response Book detailing response procedures for other cyber events. Employee security awareness training is required every six months.

Findings

F7.1 The City of Stockton does not have a formal internal policy concerning payments or procedures in ransomware attacks. This absence of policy could cause confusion, delay and greater loss of security in the event of an attack.

F7.2 The City of Stockton has a large IT Department which places cybersecurity and disaster preparedness at a high priority, minimizing risk to the City's information and service systems.

Recommendations

R7.1 By November 1, 2022, the Stockton City Council, in conjunction with the City's IT department, develop, adopt and implement a formal internal policy and procedure for response to a ransomware attack.

8.0 City of Tracy–Discussion

The City of Tracy met all expectations for cybersecurity or was in the process of meeting them when surveyed. The City has an Information Technology Division, which is part of the Finance Department. This division supports all departments and functions of the City except water treatment. Data confidentiality and security are guaranteed with industry-leading, next-generation firewalls and network access controls. Data storage, backup and cybersecurity are monitored continually. The IT Manager meets every two weeks with all other City department heads to address IT issues, including cybersecurity.

Tracy does not require encryption of thumb drives used on City devices, a requirement that is considered a "best practice" by an expert witness.

Tracy does not have either a formal Business Continuity Plan or Disaster Preparedness Plan in place but is in the process of developing both. The BCP was scheduled to be complete in April 2022. Completion date for the DPP was not specified by the City.

Findings

F8.1 Lacking a requirement for encryption of thumb drives used on City devices exposes the City of Tracy to potential data theft and contamination.

F8.2 The City of Tracy lacks a completed Business Continuity Plan, rendering Tracy relatively unprepared to restore essential services in a disruptive event.

F8.3 The City of Tracy lacks a completed Disaster Preparedness Plan, leaving Tracy at risk for delay and cost to restore IT systems in the event of a disaster.

Recommendations

R8.1 By November 1, 2022, the Tracy City Council, in conjunction with the IT division, develop, adopt and implement a policy requiring encryption of thumb drives used on City devices.

R8.2 By January 1, 2023, the Tracy City Council, in conjunction with the IT division, develop, adopt and implement a formal Business Continuity Plan.

R8.3 By January 1, 2023, the Tracy City Council provide the Grand Jury with an updated formal Disaster Preparedness Plan.

Conclusion

San Joaquin County is well protected regarding cybersecurity. The seven cities in the county vary with respect to Grand Jury expectations, most being well secured but lacking defined plans for Business Continuity and IT Disaster Preparedness. Cybersecurity is an evolving concern and requires ongoing efforts by government entities to remain current and vigilant against risks to their Information Systems.

In this investigation the Grand Jury learned from cybersecurity experts that three key elements lead to maximum agency cybersecurity:

- a dedicated information security position within each organization,
- a "seat at the table" with other agency department heads in regular meetings, and
- a rigorous employee education and training program in cybersecurity matters.

Disclaimers

Grand Jury reports are based on documentary evidence and the testimony of sworn or admonished witnesses, not on conjecture or opinion. However, the Grand Jury is precluded by law from disclosing such evidence except upon the specific approval of the Presiding Judge of the Superior Court, or another judge appointed by the Presiding Judge (Penal Code Section 911. 924.1 (a) and 929). Similarly, the Grand Jury is precluded by law from disclosing the identity of witnesses except upon an order of the court for narrowly defined purposes (Penal Code Sections 924.2 and 929).

Response Requirements

California Penal Code Sections 933 and 933.05 require that specific responses to all findings and recommendations contained in this report be submitted to the Presiding Judge of the San Joaquin County Superior Court within 90 days of receipt of the report.

The San Joaquin County Board of Supervisors and the City Councils of each city addressed shall respond to all findings and recommendations specific to their city.

Mail or hand deliver a hard copy of the response to:

Honorable Michael D. Coughlan, Presiding Judge
San Joaquin County Superior Court
180 E Weber Ave, Suite 1306J
Stockton, California 95202

Also, please email a copy of the response to Ms. Trisa Martinez, Staff Secretary to the Grand Jury, at grandjury@sjcourts.org

Attachment B

City of Lathrop

Office of the City Attorney

390 Towne Centre Drive-Lathrop, CA 95330
Phone 209-941-7235 Fax 209-941-7233
www.ci.lathrop.ca.us

September 13, 2022

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

Re: Response to Grand Jury Final Report Case No. 0321 (2021/2022).
Report received by the City of Lathrop on June 15, 2022

Honorable Michael D. Coughlan,

Pursuant to Penal Code Section 933 and 933.05, this letter is to inform you that on September 12, 2022 at a regularly scheduled City Council Meeting, the City Council of the City of Lathrop reviewed and approved the above referenced Grand Jury Final Report and directed me to write this letter of response on their behalf.

The 2021/2022 Grand Jury Final Report found that:

> Grand Jury Finding F3.1: "The City of Lathrop does not employ multi-factor authentication universally, leaving City systems more vulnerable to the activities of bad actors."
>
> Grand Jury Recommendation R3.1: "By November 1, 2022, the Lathrop City Council, in conjunction with the City's IT department, develop, adopt and implement a procedure for universal multi-factor authentication for access to City data."
>
> City Council Response: The City of Lathrop City Council agrees with Grand Jury Finding F3.1 and Recommendation R3.1 and multi-factor authentication security has been implemented and in effect since June of 2022.
>
> Grand Jury Finding F3.2: "The City of Lathrop provides an unsecured public Wi-Fi network. Misuse of this unsecured network could expose the City to liability risks."

Grand Jury Recommendation R3.2: "By November 1, 2022, the Lathrop City Council, in conjunction with the City's IT department, provide a secure public Wi-Fi network."

City Council Response: The City of Lathrop disagrees with Grand Jury Finding F3.2 and Recommendation R3.2 because by definition, publicly available Wi-Fi is inherently "unsecured", although this designation is a misnomer because it eludes to an idea that publicly available Wi-Fi can either be secured or unsecured, and that unsecured is less "safe" or more "risky" than secured. Neither are the case. An "unsecured network" only means that such Wi-Fi is publicly available for anyone to use. Wi-Fi networks, either secured or unsecured, cannot merge end-users between those networks. Secured and unsecured networks, and the end-users utilizing either, remain completely isolated from one another; it would be unfeasible for someone with access to only an unsecured Wi-Fi network to also have the ability to gain access to a separate, secured Wi-Fi network.

The commonly perpetuated idea of "risk" associated with the use of an unsecured Wi-Fi network incorrectly shapes such "risk" as something that happens upon an end-user regardless of their use of the unsecured Wi-Fi network, when in reality, risk can develop and potentially increases the more limited an end-user's understanding of how their digital presence on the internet affects their vulnerability and security. End-users should be encouraged to utilize personal checks and balances to verify the Wi-Fi networks they choose to connect to are verifiable and reputable, that their presence on the internet is not made easily available to be tracked by others, and that they are visiting legitimate websites, in order to further maintain security of their personal data and information.

Publicly available Wi-Fi is a critical asset to cities around the country. Publicly available Wi-Fi provides the public the opportunity to connect to critical and important information equitably and provides a consistent source of access to such information, promoting economic inclusion within the community. The City of Lathrop currently hosts an unsecured public Wi-Fi network entitled "City of Lathrop Guest Cloud 1" and end-users who connect to this network to access the internet must agree to the terms and conditions of its use, and which the public is only able to remain connected to for time increments of thirty (30) minute, between 7am and 7pm, seven (7) days per week.

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 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.

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 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.

Grand Jury Finding F3.5: "The City of Lathrop does not have an insurance policy covering financial losses from a cyberattack, possibly exposing City financial resources."

Grand Jury Recommendation R3.5: "By January 1, 2023, the Lathrop City Council, in conjunction with the City's IT department, obtain an insurance policy to mitigate fiscal impact resulting from cyberattack or other critical information system loss."

City Council Response: The City of Lathrop City Council partially agrees with Grand Jury Finding F3.5 and Recommendation R3.5 and would like to further clarify that staff confirmed that the City of Lathrop does in fact have cybersecurity insurance coverage, and is currently in discussions with Risk Management to enhance said coverage.

Respectfully submitted,

Salvador V. Navarrete
City Attorney

SVN/trb
Cc: Trisa Martinez at grandjury@sjcourts.org

Attachment C

City of Lathrop

DRAFT

Office of the City Attorney

390 Towne Centre Drive
Lathrop, CA 95330
Phone 209-941-7235
www.ci.lathrop.ca.us

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

Attachment D

DRAFT

Incident Response Plan

Version History

Version	Date	Author	Reason/Comments
1.8	March 2023		Document Origination

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.

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

Attachment E

DRAFT

City of Lathrop Information Security Policy

Version History

Version	Date	Author	Reason/Comments
1.8	March 2023		Document Origination

Table of Contents

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.

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)*
[redacted]	Information Security Risk Coordinator	CSIST Commander	[redacted]	[redacted]
[redacted]	Asset Manager	CSIST Commander	[redacted]	[redacted]
[redacted]	Infrastructure Manager	CSIST Manager	[redacted]	[redacted]
[redacted]	CIO	CIO	[redacted]	[redacted]
[redacted]	Communications Manager	CSIST member	[redacted]	[redacted]
[redacted]	Legal	CSIST member	[redacted]	[redacted]
[redacted]	Risk Manager	CSIST member	[redacted]	[redacted]
[redacted]	HR Representative	CSIST member	[redacted]	[redacted]
[redacted]	Physical Security Representative	CSIST member	[redacted]	[redacted]
[redacted]	3rd Party Support		[redacted]	[redacted]
[redacted]	[redacted]		[redacted]	[redacted]
FBI	Regulatory/Government Reporting Body		[redacted]	[redacted]

*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*.

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 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:

[redacted]

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

Phase I – Organizational Security

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

[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]

[redacted]

Phase II – Functional Responsibilities

The City of Lathrop CIO is responsible for:

[redacted]

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 Rick Coordinator (*tf*);

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;

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;

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:

[redacted]

Phase IV – Information Risk Management

The City of Lathrop shall maintain:

[redacted]

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.

[redacted]

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.

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] 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]

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]

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:

[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:

[redacted]

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.[redacted]

[redacted]

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

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 Department Supervisors 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.

b. The Cyber Security Incident Response Team must be notified [redacted] 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.

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 <u>must not</u> 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]

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]

[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]

[redacted]

[redacted]

[redacted]

[redacted] or

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:

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.

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.

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]

[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.

[redacted]

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.

[redacted]

[redacted]

[redacted]

[redacted]

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

[redacted]

2. [redacted]

[redacted]

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

[redacted]

Reference

Appendix I: Security Awareness References

[redacted]

[redacted]

Information Security Policy

CITY OF LATHROP ADMINISTRATIVE REGULATION 00-17

Acceptable Use of Technology

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.

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.

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.

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.

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]

____________________ Requestor Signature

__________ Date

____________________ City of Lathrop CIO Signature

__________ Date

[redacted]

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)*
[redacted]	Information Security Risk Coordinator	CSIST Commander	[redacted]	[redacted]
[redacted]	Asset Manager	CSIST Commander	[redacted]	[redacted]
[redacted]	Infrastructure Manager	CSIST Manager	[redacted]	[redacted]
[redacted]	CIO	CIO	[redacted]	[redacted]
[redacted]	Communications Manager	CSIST member	[redacted]	[redacted]
[redacted]	Legal	CSIST member	[redacted]	[redacted]
[redacted]	Risk Manager	CSIST member	[redacted]	[redacted]
[redacted]	HR Representative	CSIST member	[redacted]	[redacted]
[redacted]	Physical Security Representative	CSIST member	[redacted]	[redacted]
[redacted]	3rd Party Support		[redacted]	[redacted]
[redacted]	[redacted]		[redacted]	[redacted]
FBI	Regulatory/Government Reporting Body		[redacted]	[redacted]

*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 Team Members

Updated March 2023

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

Attachment F

DRAFT

City of Lathrop Business Continuity-Disaster Recovery Plan

Version History

Version	Date	Author	Reason/Comments
1.5	March 2023		Document Origination

Table of Contents

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.

[redacted]

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

[redacted]

Adverse Events Definition

[redacted]

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. [redacted]

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]

- 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

[redacted]

Contact Information[+]

Updated March 2023

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

*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.

[redacted]

- 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	[redacted]	Business Continuity Manager
2	[redacted]	Network SME
3	[redacted]	Network SME
4	[redacted]	Senior IT Staff
5	[redacted]	Systems Engineer
6	[redacted]	Business Continuity Team Member - Recorder
7	[redacted]	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

[redacted]

4. Disaster Recovery Strategy

[redacted]

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

Phase I – Disaster Detection and Determination

[redacted]

[redacted]

Phase II – Notification of Personnel Responsible for Recovery

When a situation occurs that could result in interruption of processing [redacted]

- The Business Continuity Manager[1]
- The Business Continuity Team[1]

[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:** [redacted]

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 [redacted] Infrastructure Manager and Communications Manager.

[redacted]

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; [redacted] is the predefined number established as the voice mail information number for posting recovery status and information notices. [redacted]

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] 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.
3.

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

[redacted]

CITY OF LATHROP, CALIFORNIA
INCORPORATED 1989

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
Contact Information	
Table 1: City of Lathrop Business Continuity Team Members	

Contact Information

Updated March 2023

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

*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	[redacted]	Business Continuity Manager
2	[redacted]	Network SME
3	[redacted]	Network SME
4	[redacted]	Senior IT Staff
5	[redacted]	Systems Engineer
6	[redacted]	Business Continuity Team Member - Recorder
7	[redacted]	Business Continuity Team Member - Recorder