Release Notes May 2025

Protected Information: May 2025

This policy has been updated because a new **Cybersecurity Policy** has been added to your manual. Changes to this policy include:

- In **SECURITY OF PROTECTED INFORMATION**, coordination requirements and a policy reference have been added.

Records Maintenance and Release: May 2025

This policy has been updated because a new **Cybersecurity Policy** has been added to your manual. Changes to this policy include:

- In **SECURITY BREACHES**, a notification requirement and a policy reference have been added.

Cybersecurity: May 2025

New Policy

This new policy has been developed to provide guidance on protecting your information technology infrastructure from cyber threats. Highlights include:

- **INFORMATION SECURITY OFFICER (ISO) RESPONSIBILITIES** outlines the ISO's responsibilities regarding oversight of the city/county's cybersecurity efforts, including but not limited to developing procedures; conducting risk assessments; developing and implementing an incident response plan; and ensuring protocols are in place for vendors and contractors.
- **EMPLOYEE AND ELECTED OFFICIAL RESPONSIBILITIES** specifies that cybersecurity efforts are the responsibility of all employees.
- **ACCESS CONTROL, PASSWORD, AND USER MANAGEMENT** outlines the levels of appropriate access and what shall be done upon an employee's separation from employment.
- **INCIDENT RESPONSE PLAN** outlines what procedures for the plan should include.
- **CYBERSECURITY TRAINING PROGRAM** specifies that training is required for all employees and elected officials and outlines what the training program should include

Information Technology Use: May 2025

This policy has been updated because a new **Cybersecurity Policy** has been added to your manual. Changes to this policy include:

- In **PURPOSE AND SCOPE**, a policy reference has been added.
- In **PROTECTION OF SYSTEMS AND FILES**, reporting requirements have been updated.

Generative Artificial Intelligence Use: May 2025

This policy has been updated because a new **Cybersecurity Policy** has been added to your manual. Changes to this policy include:

- In **PURPOSE AND SCOPE**, a policy reference has been added.
- In **AI COORDINATOR**, content has been updated for clarity and to include a coordination requirement.

Purchasing and Procurement: May 2025

New Policy

This new policy has been developed in response to customer feedback to provide guidance on the purchasing and procurement of goods and services. Highlights include:

- **POLICY** establishes that all purchase and procurement activities will be conducted in a manner that maintains public trust.
- **PROCUREMENT SERVICES MANAGER** outlines specific responsibilities for the position.
- **AUDITS** provides requirements for an annual audit and periodic reviews.
- **RECORDS** outlines requirements in accordance with the record retention schedule.

Protected Information

501.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the access, transmission, release, and security of protected information by employees of the City. This policy addresses the protected information that is used in the day-to-day operation of the City and not the public records information covered in the Records Maintenance and Release Policy.

501.1.1 DEFINITIONS

Definitions related to this policy include:

Protected information - Any information or data that is collected, stored, or accessed by employees of the City and is subject to any access or release restrictions imposed by law, regulation, order, or use agreement. This includes all information contained in federal, state, or local databases that is not accessible to the public.

501.2 POLICY

Employees of the City will adhere to all applicable laws, orders, regulations, use agreements, and training related to the access, use, dissemination, and release of protected information.

501.3 RESPONSIBILITIES

The City Manager designates the City Secretary to coordinate the use of protected information, including:

(a) Overseeing employee compliance with this policy and with requirements applicable to protected information.

(b) Developing, disseminating, and maintaining procedures necessary to comply with any requirements for the access, use, dissemination, release, and security of protected information.

(c) Developing procedures to ensure training and certification requirements are met.

(d) Resolving specific questions that arise regarding authorized recipients of protected information.

(e) Implementing security practices and procedures to comply with requirements applicable to protected information.

501.4 ACCESS TO PROTECTED INFORMATION

Protected information shall not be accessed in violation of any law, order, regulation, use agreement, city policy, or training. Only those employees who have completed applicable training and met any applicable requirements, such as a background check, may access protected information, and only when the employee has a legitimate work-related reason for such access.

Unauthorized access, including access for other than a legitimate work-related purpose, is prohibited.

501.5 RELEASE OR DISSEMINATION OF PROTECTED INFORMATION

Protected information may be released only to authorized recipients who have both a lawful right to know and need to know.

An employee who is asked to release protected information that should not be released should refer the requesting person the City Secretary for information regarding a formal request.

501.6 SECURITY OF PROTECTED INFORMATION

The City Manager ~~designates~~ should designate an employee of the City ~~Secretary~~ to oversee the security of protected information, including:

(a) ~~Developing and maintaining~~ Coordinating with the Information Security Officer (ISO) to develop and maintain security practices, procedures, and training.

(b) Maintaining compliance with any federal, state, and local requirements pertaining to the security of protected information.

(c) Establishing procedures to provide for the preparation, prevention, detection, analysis, and containment of security incidents, including cyberattacks.

(d) Tracking, documenting, and reporting all breach of security incidents pursuant to the incident reporting procedures established by the ISO, where applicable, the City Manager, and appropriate authorities (see the Cybersecurity Policy).

501.6.1 EMPLOYEE RESPONSIBILITIES

Employees accessing or receiving protected information shall ensure the information is not accessed or received by persons who are not authorized to access or receive it. This includes not leaving protected information, such as documents or computer databases, accessible to others when it is reasonably foreseeable that unauthorized access may occur (e.g., on an unattended table or desk, in or on an unattended vehicle, in an unlocked desk drawer or file cabinet, on an unattended computer terminal).

501.7 TRAINING

All employees authorized to access or release protected information shall complete a training program that complies with any protected information system requirements and identifies authorized access and use of protected information, as well as its proper handling and dissemination.

Records Maintenance and Release

500.1 PURPOSE AND SCOPE

This policy provides guidance on the maintenance and release of city records. Protected information is separately covered in the Protected Information Policy.

500.2 POLICY

The City is committed to providing public access to records in a manner that is consistent with state public records laws.

500.3 CITY SECRETARY

The City Manager shall designate a City Secretary. The responsibilities of the City Secretary include but are not limited to:

(a) Managing the records management system for the City, including the retention, archiving, release, and destruction of city public records.

(b) Maintaining and updating the city records retention schedule, including:

1. Identifying the minimum length of time records must be kept.
2. Identifying the city department responsible for the original record.

(c) Establishing rules regarding the inspection and copying of public records as reasonably necessary for the protection of such records.

(d) Identifying records or portions of records that are confidential under state or federal law and not open for inspection or copying.

(e) Establishing rules regarding the processing of subpoenas for the production of records.

(f) Ensuring the availability of a current schedule of fees for public records as allowed by law.

(g) Preparing and making available to the public the records request process, to include the cost of inspecting or obtaining copies.

500.4 PROCESSING REQUESTS FOR PUBLIC RECORDS

Any employee who receives a request for any record shall route the request to the City Secretary or the authorized designee.

500.4.1 REQUESTS FOR RECORDS

The processing of requests for any record is subject to the following:

(a) All requests should be made in writing or on a form supplied by the City.

(b) Clarification may be sought if the request is unreasonably broad or unclear.

(c) Inspection of records should be during regular business hours unless otherwise authorized by the City Secretary.

(d) Records should be made available in a format readily accessible to the requester. Records may also be made available in a specific format requested and a fee charged for reasonable costs of any required processing.

(e) Records should be provided or a denial provided to a requester within a reasonable period of time.

1. If a delay in providing records is anticipated, the requester should be provided a written response with the reason for the delay and the anticipated date the records will be provided.

(f) Fees should be charged as allowed by law and established by the City.

(g) The City is not required to create records that do not exist.

(h) When a record contains material with release restrictions and material that is not subject to release restrictions, the restricted material shall be redacted and the unrestricted material released.

1. A copy of the redacted release should be maintained in the city file for proof of what was actually released and as a place to document the reasons for the redactions. If the record is audio or video, a copy of the redacted audio/video release should be maintained in the city-approved media storage system and a notation should be made in the file to document the release and the reasons for the redacted portions.

500.4.2 DENIALS

The denial of a request for records should be documented and include:

(a) A description of the records requested.

(b) The specific reasons for the denial.

(c) The name, title, and signature of the City Secretary.

(d) The procedure to appeal the denial.

500.5 RELEASE RESTRICTIONS

Examples of release restrictions include:

(a) Any personal identifying information, including an individual's photograph; Social Security and driver identification numbers; name, address, and telephone number; and medical or disability information that is contained in any city record, except as authorized by the City, and only when such use or disclosure is permitted or required by law to carry out a legitimate government purpose.

(b) Certain personnel information, including but not limited to an employee's residential address and telephone number, Social Security number, marital status, medical history, confidential recommendations for employment, and performance evaluation history.

(c) Records pertaining to internal investigations and disciplinary matters, including but not limited to complaints and other records relating to allegations of discrimination,

harassment, or retaliation, until the investigation is complete or is made part of the official record of any hearing or court proceeding.

(d) Certain 9-1-1 records.

(e) Audio and video recordings obtained through use of body-worn cameras by law enforcement officers, except as provided by statute.

(f) Certain concealed firearm license/permit information of an applicant.

(g) Records concerning security plans, procedures, assessments, measures, or systems, and other records relating to the security of persons, structures, facilities, infrastructure, or information technology systems that could reasonably be expected to be detrimental to the public's safety or welfare.

(h) Records pertaining to strategy or negotiations related to labor relations, employment contracts, or collective bargaining and related arbitration proceedings.

(i) Drafts, notes, recommendations, or intra-governmental memorandums pertaining to the development of resolutions, regulations, statements of policy, management directives, ordinances, or amendments prepared by or for the City.

(j) Records where disclosure would be detrimental to the best interests of the public.

(k) Records pertaining to pending or potential litigation that are not records of any court.

(l) Any other information that may be appropriately denied by federal or state law.

500.6 SUBPOENAS AND DISCOVERY REQUESTS

Any employee who receives a subpoena duces tecum or discovery request for records should promptly contact a supervisor and the City Secretary for review and processing. While a subpoena duces tecum may ultimately be subject to compliance, it is not an order from the court that will automatically require the release of the requested information.

Generally, discovery requests and subpoenas should be referred to the City Manager or the authorized designee.

All questions regarding compliance with any subpoena duces tecum or discovery request should be promptly referred to the City Manager or legal counsel so that a timely response can be prepared.

500.7 RELEASED RECORDS TO BE MARKED

Each page of any written record released pursuant to this policy should be stamped in a colored ink or otherwise marked to indicate the city name and to whom the record was released.

Each audio/video recording released should include the city name and to whom the record was released.

500.8 SECURITY BREACHES

Employees who become aware that any city records system may have been breached should notify the City Secretary as soon as practicable.

The City Secretary shall ensure any required notice of the breach is given.

If the breach reasonably appears to have been made to protected information covered in the Protected Information Policy, the City Secretary should promptly notify the appropriate employee designated to oversee the security of protected information (see the Protected Information Policy).

If the breach involves or may involve a cybersecurity incident, the City Secretary should immediately report it pursuant to the incident reporting procedures established by the Information Security Officer (see the Cybersecurity Policy).

500.9 EXPUNGEMENT

The City Secretary shall review all court orders and other filings that pertain to the expungement or sealing of records for appropriate action. Once a record is expunged or sealed, employees shall respond to any inquiry as though the record did not exist.

500.10 TRAINING

Employees authorized to manage, release, or facilitate public access to city records should receive training that includes identification of material appropriate for release or public access and the city systems and procedures guiding such release and access.

Cybersecurity

410.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines to protect the [city_county]'s information technology infrastructure from cyber threats.

Additional guidelines for the use of [city_county] information technology infrastructure are found in the Information Technology Use Policy.

410.1.1 DEFINITIONS

Definitions related to this policy include:

Cybersecurity – The practice of protecting an information technology infrastructure from digital attacks.

Cybersecurity incident - Any incident that compromises the security of the information technology infrastructure of the [city_county]. This includes but is not limited to data breaches, unauthorized access attempts, malware infections, phishing attacks, and any other suspicious activity.

Cyber threats – Unauthorized access, use, disclosure, disruption, modification, or destruction of the [city_county]'s information technology infrastructure.

Information technology infrastructure – All electronic devices, networks, systems (e.g., hardware, software, firmware), and data owned, operated, or managed by the [City_County], including but not limited to computers, servers, mobile devices, networking equipment, and cloud-based services.

410.2 POLICY

The [City_County] is committed to maintaining the security and integrity of its information technology infrastructure and will take reasonable cybersecurity measures to safeguard its information technology infrastructure from cyber threats.

410.3 [CM_CA] RESPONSIBILITIES

The [CM_CA] is responsible for securing and allocating the necessary resources, support, and guidance to provide effective cybersecurity measures.

The [CM_CA] shall appoint an Information Security Officer (ISO) to oversee and implement the [city_county]'s cybersecurity efforts. The ISO should report directly to the [CM_CA].

The [CM_CA] should ensure that the appointed ISO receives appropriate training and maintains appropriate credentials needed to complete the assigned job responsibilities.

410.4 INFORMATION SECURITY OFFICER (ISO) RESPONSIBILITIES

Responsibilities of the ISO include but are not limited to:

(a) Overseeing the [city_county]'s cybersecurity efforts. This includes assessing and implementing appropriate cybersecurity technologies, including firewalls, antivirus software, intrusion detection systems, and data encryption tools.

(b) Developing procedures related to specific [city_county] cybersecurity efforts, such as acceptable use, password management, and remote access.

(c) Remaining familiar with and facilitating [city_county] compliance with all applicable and emerging federal, state, and local laws related to cybersecurity, such as the Federal Information and Security Modernization Act (FISMA) (44 USC § 3551 et. seq.) and the Cybersecurity Information Sharing Act (CISA) (6 USC § 1501 et. seq.).

(d) Conducting periodic risk assessments to identify potential vulnerabilities in the [city_county]'s information technology infrastructure.

1. The risk assessment should include a review of the [city_county]'s cybersecurity technologies to address emerging threats, as appropriate.

(e) Developing and implementing risk mitigation strategies based on the findings of the risk assessment, including updates to the [city_county]'s cybersecurity technologies.

(f) Developing and maintaining procedures for data protection, including classifying data based on the sensitivity of the data, performing data backups, and securely disposing of sensitive data.

(g) Developing and implementing procedures for employees and elected officials to report suspected or potential cybersecurity incidents.

(h) Developing and implementing an incident response plan to address potential cybersecurity breaches or attacks.

(i) Coordinating with the training manager to develop and implement a comprehensive cybersecurity training program for all employees and elected officials.

(j) Responding to and advising employees and elected officials on cybersecurity questions or issues related to [city_county] cybersecurity practices.

(k) Coordinating with [city_county] [dept_div_agency] staff and [DepartmentHead]s to ensure compliance with this policy.

(l) Ensuring that protocols are in place to require all vendors and contractors handling [city_county] data to adhere to this policy's cybersecurity standards and any and all procedures or practices established by the ISO. This may be accomplished by including provisions for data protection, breach reporting, and secure data handling practices in contractual agreements.

(m) Regularly reviewing this policy and related policies or procedures and recommending amendments as needed.

410.5 EMPLOYEE AND ELECTED OFFICIAL RESPONSIBILITIES

All [City_County] employees and elected officials share responsibility for proactively protecting the [city_county] information technology infrastructure from cyber threats and cybersecurity incidents.

Employees and elected officials shall immediately report any suspicious activity, actual or suspected cyber threats, or cybersecurity incidents pursuant to the procedures established by the ISO.

410.6 ACCESS CONTROL, PASSWORD, AND USER MANAGEMENT

Access to [city_county] information technology infrastructure shall be granted based on the principle of least privilege so that [city_county] employees have only the necessary access rights required for their specific job duties.

The [city_county] shall require password access to the [city_county] information technology infrastructure. Passwords shall be required to meet the minimum length and complexity requirements, be changed periodically, and not be shared, reused, or stored in plain text. The [City_County] shall implement multi-factor authentication for systems containing sensitive or critical information.

Upon separation from employment, an employee's access to the [city_county] information technology infrastructure shall be immediately terminated.

410.7 NETWORK SECURITY

The [City_County] shall implement firewalls and other intrusion prevention systems to protect the [city_county] information technology infrastructure from unauthorized access, malware, and other cyber threats.

The [City_County] shall ensure that [city_county] wireless networks are secured using encryption, strong passwords, firewall configurations, and any additional security protocols necessary to protect against cyber threats.

Information systems shall be configured securely to protect the security of [city_county] data.

410.8 DATA CLASSIFICATION, PROTECTION, AND DISPOSAL

Data should be classified by the [City_County] based on its sensitivity. Appropriate security controls should be implemented based on the classification level of the data.

Regular data backups shall be performed by the [city_county] and shall be stored in a secure location. The process used for data backup and recovery shall be regularly tested to confirm it can adequately recover data if needed. All testing should be documented.

The ISO shall also ensure that sensitive data at rest and in transit is encrypted using industry standard encryption algorithms and protocols.

The disposal of sensitive information should follow appropriate protocols to prevent unauthorized retrieval (e.g., secure erasure, destruction of data).

410.9 INCIDENT RESPONSE PLAN

The [City_County] should maintain an incident response plan that addresses cybersecurity incidents promptly. The incident response plan should include procedures for:

(a) The receipt and processing of reported cybersecurity incidents or events.

(b) Specific steps for identifying, containing, and mitigating security incidents.

(c) Coordination with relevant departments, external agencies, and other stakeholders to develop an appropriate response.

(d) Regular audits to determine compliance with incident response procedures.

(e) Post-incident recovery actions and protocols, including:

1. Containment and eradication of threat.
2. Recovery of data.
3. Required reporting.
4. Continuity of services.

(f) The investigation of any reported cybersecurity incidents, including steps to prevent future occurrences.

(g) Regular interactive simulations and practical exercises to test compliance and awareness of incident response procedures.

410.10 CYBERSECURITY TRAINING PROGRAM

All employees and elected officials shall complete initial and annual cybersecurity awareness training consistent with the requirements established in the cybersecurity training program.

The cybersecurity training program should include instruction on the following:

(a) Recognizing and avoiding threats (e.g., phishing awareness, social engineering tactics, safe browsing).

(b) Secure device use (e.g., keeping devices updated and secure, mobile device security, physical device security).

(c) Safe network practices (e.g., Wi-Fi security considerations, virtual private networks, firewall and antivirus software).

(d) Data security (e.g., data encryption and backup, handling confidential data).

(e) This policy and all related policies and procedures, including:

1. Acceptable use, password protection, and remote access procedures.
2. Procedures for data classification.
3. Incident reporting procedures.
4. Incident response plans.
5. Applicable state and federal law related to cybersecurity.

Information Technology Use

201.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the proper use of city information technology resources, including computers, electronic devices, hardware, software, and systems.

Additional guidelines for the use of city information technology resources are found in the Cybersecurity Policy.

201.1.1 DEFINITIONS

Definitions related to this policy include:

Computer system - All computers (on-site and portable), electronic devices, hardware, software, and resources owned, leased, rented, or licensed by the City that are provided for official use by its employees. This includes all access to, and use of, Internet Service Providers (ISP) or other service providers provided by or through the City or city funding.

Hardware - Includes but is not limited to computers, computer terminals, network equipment, electronic devices, telephones (including cellular and satellite), pagers, modems, or any other tangible computer device generally understood to comprise hardware.

Software - Includes but is not limited to all computer programs, systems, and applications, including shareware. This does not include files created by the individual user.

Temporary file, permanent file, or file - Any electronic document, information, or data residing or located, in whole or in part, on the system, including but not limited to spreadsheets, calendar entries, appointments, tasks, notes, letters, reports, messages, photographs, or videos.

201.2 POLICY

It is the policy of the City that employees shall use information technology resources, including computers, software, and systems, that are issued or maintained by the City in a professional manner and in accordance with this policy.

201.3 PRIVACY EXPECTATION

Employees forfeit any expectation of privacy with regard to emails, texts, or anything published, shared, transmitted, or maintained through file-sharing software or any internet site that is accessed, transmitted, received, or reviewed on any city computer system.

The City reserves the right to access, audit, and disclose, for whatever reason, any message, including attachments, and any information accessed, transmitted, received, or reviewed over any technology that is issued or maintained by the City, including the city email system, computer network, and/or any information placed into storage on any city system or device. This includes records of all key strokes or web-browsing history made at any city computer or over any city network. The fact that access to a database, service, or website requires a username or password

will not create an expectation of privacy if it is accessed through city computers, electronic devices, or networks.

201.4 RESTRICTED USE

Employees shall not access computers, devices, software, or systems for which they have not received prior authorization or the required training. Employees shall immediately report unauthorized access or use of computers, devices, software, or systems by another employee to their supervisors.

Employees shall not use another person's access passwords, logon information, and other individual security data, protocols, and procedures unless directed to do so by a supervisor.

201.4.1 SOFTWARE

Employees shall not copy or duplicate any copyrighted or licensed software except for a single copy for backup purposes, in accordance with the software company's copyright and license agreement.

To reduce the risk of a computer virus or malicious software, employees shall not install any unlicensed or unauthorized software on any city computer. Employees shall not install personal copies of any software on any city computer.

No employee shall knowingly make, acquire, or use unauthorized copies of computer software that is not licensed to the City while on city premises, computer systems, or electronic devices. Such unauthorized use of software exposes the City and involved employees to severe civil and criminal penalties.

Introduction of software by employees should only occur as a part of the automated maintenance or update process of city-approved or installed programs by the original manufacturer, producer, or developer of the software. Any other introduction of software requires prior authorization from a supervisor and a full scan for malicious attachments.

201.4.2 HARDWARE

Access to technology resources provided by or through the City shall be strictly limited to city-related activities. Data stored on or available through city computer systems shall only be accessed by authorized employees who have a legitimate city-related purpose to access such data. Any exceptions to this policy must be approved by a supervisor.

201.4.3 INTERNET USE

Internet access provided by or through the City shall be strictly limited to city-related activities. Internet sites containing information that is not appropriate or applicable to city use and that shall not be intentionally accessed include but are not limited to adult forums, pornography, gambling, chat rooms, and similar or related internet sites. Certain exceptions may be permitted with the express approval of a supervisor as a function of an employee's assignment.

Downloaded information from the internet shall be limited to messages, mail, and data files.

201.4.4 USE DURING NON-WORK HOURS

Employees shall only use technology resources provided by the City during work hours unless specifically authorized by a supervisor. This includes the use of telephones, cell phones, texting, email, or any other off-the-clock work-related activities. This also applies to personally owned devices that are used to access city resources.

Refer to the Personal Communication Devices Policy for guidelines regarding use of personally owned technology during non-work hours.

201.5 PROTECTION OF SYSTEMS AND FILES

All employees have a duty to protect the computer system and related systems and devices from physical and environmental damage and are responsible for the correct use, operation, care, and maintenance of the computer system.

Employees shall ensure city computers and access terminals are not viewable by unauthorized users. Computers and terminals should be secured, users logged off, and password protections enabled whenever the user is not present. Access passwords, logon information, and other individual security data, protocols, and procedures are confidential information and are not to be shared. Password length, format, structure, and content shall meet the prescribed standards required by the computer system or as directed by a supervisor and shall be changed at intervals as directed.

It is prohibited for an employee to allow an unauthorized user to access the computer system at any time or for any reason. Employees shall ~~promptly~~ immediately report any unauthorized access to the computer system or suspected intrusion from outside sources (including the internet) ~~to a supervisor~~ pursuant to the incident reporting procedures established by the Information Security Officer.

201.6 INSPECTION AND REVIEW

A supervisor or the authorized designee has the express authority to inspect or review the computer system, all temporary or permanent files, related electronic systems or devices, and any contents thereof, whether such inspection or review is in the ordinary course of supervisory duties or based on cause.

Reasons for inspection or review may include but are not limited to computer system malfunctions, problems, or general computer system failure, a lawsuit against the City involving one of its employees or an employee's duties, an alleged or suspected violation of any city policy, a request for disclosure of data, or a need to perform or provide a service.

Qualified staff may extract, download, or otherwise obtain any and all temporary or permanent files residing or located in or on the city computer system when requested by a supervisor or during the course of regular duties that require such information.

Generative Artificial Intelligence Use

407.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for city use of generative artificial intelligence (GenAI). This policy does not apply to artificial intelligence that is integrated into facial recognition applications, voice recognition applications, biometric access controls, or software that redacts documents or video or similar applications.

Additional guidelines for the use of city information technology resources are found in the Information Technology Use ~~Policy~~ and Cybersecurity policies.

407.1.1 DEFINITIONS

Definitions related to this policy include:

Generative artificial intelligence (GenAI) - A type of artificial intelligence that is algorithmically trained on one or more large data sets and designed to generate new and unique data (e.g., text, pictures, video) in response to a prompt (generally questions, instructions, images, or video) input by the user.

407.2 POLICY

The use of GenAI systems carries unique benefits within a local government entity, providing ways to increase operational efficiency, enhance city procedures, and improve the overall effectiveness of the City.

However, the prompts input into GenAI systems can present risks to both individuals and local governments by making accessible to the public information such as facility security records, security procedures, personal information, certain law enforcement records, and other confidential information (e.g., protected information, social services records, financial records). In addition, without safeguards in place, GenAI can produce unintended discriminatory or biased output as well as content that is inaccurate, misleading, or copyrighted.

It is the policy of the City to develop, implement, and use GenAI ethically and responsibly in a way that minimizes potential risk and harm in accordance with the guidelines set forth below.

Any function carried out by an employee of the City using GenAI is subject to the same laws, rules, and policies as if carried out without the use of GenAI. The use of GenAI does not permit any law, rule, or policy to be bypassed or ignored.

407.3 RESPONSIBILITIES

407.3.1 CITY MANAGER

The City Manager or an authorized designee shall approve all GenAI systems, their acceptable uses, and their authorized user groups prior to the use, implementation, or development for any city functions.

407.3.2 AI COORDINATOR

The City Manager or the authorized designee shall appoint an AI coordinator. The AI coordinator shall report to the City Manager or the authorized designee.

The responsibilities of the AI coordinator include but are not limited to:

(a) Evaluating potential GenAI systems and recommending those GenAI systems that appear to be appropriate and trustworthy to the City Manager or the authorized designee. The trustworthiness of GenAI systems should be evaluated by balancing the following characteristics:

1. Validity and reliability - The system's apparent ability to meet the intended purpose and fulfill the needs of the City consistently over time.
2. Safety - Any apparent risk to human life, health, property, or the environment that could result from the city's use of the system.
3. Security and resiliency - The system's capability to prevent unauthorized access and misuse and its ability to return to normal function should misuse occur.
4. Accountability and transparency - The ability to track and measure the system's use and activity through histories, audit logs, and other processes to provide insight about the system and identify potential sources of error, bias, or vulnerability.
5. Explainability and interpretability - The ability of the user to understand the purpose and impact of the system, how and why the system reached the resulting output, and what the output means for the user.
6. Privacy - The ability of the system to protect confidentiality and meet applicable privacy standards for the types of data intended to be input into the system (e.g., state privacy laws, Criminal Justice Information Services (CJIS), Health Insurance Portability and Accountability Act (HIPAA)).
7. Fairness - The ability of the system to operate in a way that avoids or minimizes bias and discrimination.

(b) Ensuring appropriate contractual safeguards are in place to manage third-party use of city data and to restrict the use of input in AI training data sets. If the input of protected information is necessary for the proper use of the GenAI system, an information-exchange agreement in compliance with applicable rules and standards (e.g., HIPAA requirements) should be used to outline the roles, responsibilities, and data ownership between the City and third-party vendor.

(c) Coordinating with the Information Security Officer and others within the City, such as the information technology or legal departments, as appropriate to ensure GenAI systems are procured, implemented, secured, and used appropriately.

(d) Maintaining a list or inventory of city-approved GenAI systems and, when appropriate for city transparency, making the list or inventory available to the public.

(e) Developing and maintaining appropriate procedures related to the use of GenAI systems, including procedures for editing and fact-checking output.

(f) Ensuring any public-facing GenAI systems notify the user that GenAI is being used.

(g) Developing and updating training for the authorized users of each city-approved GenAI system.

(h) Ensuring access to city GenAI systems is limited to authorized users and establishing requirements for user credentials such as two-factor authentication and appropriate password parameters.

(i) Conducting audits at reasonable time intervals for each of the GenAI systems utilized by the City to evaluate the performance and effectiveness of each approved system and to determine if it continues to meet the city's needs and expectations of trustworthiness. The coordinator should arrange for audits to be conducted by an external source, as needed.

(j) Ensuring each GenAI system is updated and undergoes additional training as reasonably appears necessary in an effort to avoid the use of outdated information or technologies.

(k) Keeping abreast of advancements in GenAI and any GenAI-related legal developments.

(l) Reviewing this policy and city practices and proposing updates as needed to the City Manager or the authorized designee.

407.4 USE OF GENERATIVE AI

The use of city GenAI systems by city employees shall be limited to official work-related purposes, and employees shall only access and use GenAI systems for which they have been authorized and received proper training.

Employees shall use AI-generated content as an informational tool and not as a substitution for human judgment or decision-making. Employees should not represent AI-generated content as their own original work.

AI-generated content should be considered draft material only and shall be thoroughly reviewed prior to use. Before relying on AI-generated content, employees should:

(a) Obtain independent sources for information provided by GenAI and take reasonable steps to verify that the facts and sources provided by GenAI are correct and reliable.

(b) Review prompts and output for indications of bias and discrimination and take steps to mitigate its inclusion when reasonably practicable.

(c) Include a statement in the final document or work product that GenAI was used to aid in its production.

407.4.1 PRIVACY CONSIDERATIONS

Information not otherwise available to the public, including data reasonably likely to compromise an investigation, reveal confidential security information, training, or procedures, or risk the safety of any individual if it were to become publicly accessible, should not be input into a GenAI system unless contractual safeguards are in place to prevent such information from becoming publicly

accessible. Employees should instead use generic unidentifiable inputs, such as "person," and hypothetical scenarios whenever possible.

Protected information should only be input into GenAI systems that have been approved for such use and comply with applicable privacy laws and standards (see the Protected Information Policy).

407.5 PROHIBITED USE

Employees shall not create user accounts in their official capacity or input work-related data (including information learned solely in the scope of their employment) into publicly available GenAI systems unless the system has been approved by the City Manager or the authorized designee for the intended use.

407.6 TRAINING

The AI coordinator should ensure that all members authorized to use GenAI have received appropriate initial training that is suitable for their role and responsibilities prior to their use of GenAI and receive periodic refresher training. Training should include but is not limited to the following:

(a) A review of this policy

(b) The need for human oversight of GenAI outputs

(c) The interpretation, review, and verification of GenAI output

(d) Checking GenAI output for bias or protected information

(e) Ethical use of GenAI technology

(f) Data security and privacy concerns

Purchasing and Procurement

206.1 PURPOSE AND SCOPE

This policy provides guidelines for the purchasing and procurement of goods and services for the [city_county].

206.2 POLICY

It is the policy of the [city_county] to conduct purchasing and procurement in an efficient and cost-effective manner consistent with federal, state, and local laws, rules, and requirements in order to protect the integrity of the [city_county] and maintain public trust.

206.2.1 DEFINITIONS

Definitions related to this policy include:

Goods – Any property purchased by the [City_County], including but not limited to equipment, supplies, materials, and parts.

Procurement – The acquisition of goods or services.

Services – The furnishing of labor by a contractor that includes all work or labor performed for the [city_county] on an independent contractor basis, including but not limited to maintenance, construction and personal or professional services.

Director of Finance

206.3 PROCUREMENT SERVICES MANAGER RESPONSIBILITIES

The [CM_CA] shall designate ~~an employee~~ to serve as the Procurement Services Manager to oversee purchases and procurement for the [city_county]. The responsibilities of the Procurement Services Manager include but are not limited to:

(a) Establishing rules and procedures for the [city_county]'s procurement process.

(b) Establishing procedures for employee use of [city_county] payment methods (i.e., purchasing cards, checks).

(c) Maintaining compliance with federal, state, and local purchasing and procurement laws, rules, and requirements.

(d) Reviewing proposed purchases to determine the most appropriate method of procurement.

1. If the procurement method selected is one other than competitive bidding, documenting why another method was selected.

(e) Participating in all purchases made on a competitive bid process and ensuring that all purchased supplies, materials, and equipment are delivered in accordance with the contract terms.

(f) Assisting [city_county] employees involved with purchasing and procurement of goods or services in following purchasing requirements and rules applicable to the method of procurement.

(g) Forwarding all contracts and purchase orders to the [CM_CA] or the authorized designee for review, approval, and execution.

206.4 AUDITS

The Procurement Services Manager should ensure that periodic reviews and an annual audit of purchasing and procurement activities are conducted to determine compliance with any applicable federal, state, and local laws, rules, and requirements.

206.5 RECORDS

All records created and submitted during and related to the purchasing and procurement process should be maintained in accordance with the established records retention schedule.