

## Chapter 5 - Records and Documents

## 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 CUSTODIAN OF RECORDS

The City Administrator shall designate a Custodian of Records . The responsibilities of the Custodian of Records 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 Custodian of Records 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 Custodian of Records .

## *Records Maintenance and Release*

---

- (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 Custodian of Records .
- (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,

## *Records Maintenance and Release*

---

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 Custodian of Records 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 Administrator or the authorized designee.

All questions regarding compliance with any subpoena duces tecum or discovery request should be promptly referred to the City Administrator 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 Custodian of Records as soon as practicable.

## *Records Maintenance and Release*

---

The Custodian of Records 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 Custodian of Records should promptly notify the appropriate employee designated to oversee the security of protected information (see the Protected Information Policy).

### **500.9 EXPUNGEMENT**

The Custodian of Records 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.

---

## 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 Administrator should designate an employee of the City 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.

## *Protected Information*

---

### **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 to a supervisor or to the Custodian of Records for information regarding a formal request.

### **501.6 SECURITY OF PROTECTED INFORMATION**

The City Administrator should designate an employee of the City to oversee the security of protected information, including:

- (a) Developing and maintaining 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 to the City Administrator and appropriate authorities.

#### **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.

## Personnel Records

### 502.1 PURPOSE AND SCOPE

This policy governs maintenance and access to personnel records. Personnel records include any file maintained under an individual employee's name.

### 502.2 POLICY

It is the policy of the City to maintain personnel records and preserve the confidentiality of personnel records pursuant to the Constitution and the laws of this state.

### 502.3 PERSONNEL FILE

A personnel file shall be maintained as a record of a person's employment/appointment with this city. The personnel file should contain, at a minimum:

- (a) Personal data, including photographs, marital status, names of family members, educational and employment history, or similar information.
- (b) Election of employee benefits.
- (c) Personnel action reports reflecting assignments, promotions, and other changes in employment/appointment status.
- (d) Original performance evaluations.
- (e) Discipline records, including copies of sustained personnel complaints.
- (f) Adverse comments such as supervisor notes or memos may be retained in the city file after the employee has had the opportunity to read and initial the comment.
  - 1. Once an employee has had an opportunity to read and initial any adverse comment, the employee shall be given the opportunity to respond in writing to the adverse comment.
  - 2. Any employee response shall be attached to and retained with the original adverse comment.
  - 3. If an employee refuses to initial or sign an adverse comment, at least one supervisor should note the date and time of such refusal on the original comment. Such a refusal, however, shall not be deemed insubordination, nor shall it prohibit the entry of the adverse comment into the employee's file.
- (g) Commendations and awards.
- (h) Any other information, the disclosure of which would constitute an unwarranted invasion of personal privacy.

### 502.4 DEPARTMENT, DIVISION, OR AGENCY FILE

Department files may be separately maintained internally by an employee's supervisor for the purpose of completing timely performance evaluations. The file may contain supervisor comments,

## *Personnel Records*

---

notes, notices to correct, and other materials that are intended to serve as a foundation for the completion of timely performance evaluations.

### **502.5 TRAINING FILE**

An individual training file should be maintained for each employee whose position requires specialized training or certification. Training files should contain records of all training; original or photocopies of available certificates, transcripts, diplomas, and other documentation; and education and firearms qualifications, as applicable. Training records may also be created and stored remotely, either manually or automatically.

- (a) The involved employee is responsible for providing an immediate supervisor with evidence of completed training/education in a timely manner.
- (b) Supervisors should ensure that copies of such training records are placed in the employee's training file.

### **502.6 MEDICAL FILE**

A medical file shall be maintained separately from all other personnel records and shall contain all documents relating to the employee's medical condition and history, including but not limited to

- (a) Materials relating to a medical leave of absence, including leave under the Family and Medical Leave Act (FMLA).
- (b) Documents relating to workers' compensation claims or the receipt of short- or long-term disability benefits.
- (c) Fitness-for-duty examinations, psychological and physical examinations, follow-up inquiries, and related documents.
- (d) Medical release forms, doctor's slips, and attendance records that reveal an employee's medical condition.
- (e) Any other documents or materials that reveal the employee's medical history or medical condition, including past, present, or future anticipated mental, psychological, or physical limitations.

### **502.7 SECURITY**

Personnel records should be maintained in a secured location and locked either in a cabinet or access-controlled room. Personnel records maintained in an electronic format should have adequate password protection.

Personnel records are subject to disclosure only as provided in this policy, the Records Maintenance and Release Policy, or according to applicable discovery procedures.

Nothing in this policy is intended to preclude review of personnel records by the City Administrator or representatives of the City in connection with official business.

## *Personnel Records*

---

### 502.7.1 REQUESTS FOR DISCLOSURE

Any employee receiving a request for a personnel record shall promptly notify the Custodian of Records or other person charged with the maintenance of such records.

Upon receipt of any such request, the responsible person shall notify the affected employee as soon as practicable that such a request has been made.

The responsible person shall further ensure that an appropriate response to the request is made in a timely manner, consistent with applicable law. In many cases, this may require assistance of available legal counsel.

All requests for disclosure that result in access to an employee's personnel records shall be logged in the corresponding file.

### **502.8 EMPLOYEES' ACCESS TO THEIR PERSONNEL RECORDS**

Employees may request access to their own personnel records during the normal business hours of those responsible for maintaining such files. Employees seeking the removal of any item from their personnel records should file a written request to the City Administrator. The City should remove any such item if appropriate, or within 30 days provide the employee with a written explanation of why the contested item will not be removed. If the contested item is not removed from the file, the employee's request and the written response from the City should be retained with the contested item in the employee's corresponding personnel record.

Employees may be restricted from accessing files containing certain information (e.g., ongoing investigations to the extent that it could jeopardize or compromise the investigation).

### **502.9 RETENTION AND PURGING**

Personnel records shall be maintained in accordance with the established records retention schedule:

- (a) During the preparation of each employee's performance evaluation, all personnel complaints and disciplinary actions should be reviewed to determine the relevancy, if any, to progressive discipline, training, and career development. Each supervisor responsible for completing the employee's performance evaluation should determine whether any prior sustained disciplinary file should be retained beyond the required period for reasons other than pending litigation or other ongoing legal proceedings.
- (b) If a supervisor determines that records of prior discipline should be retained beyond the required period, approval for such retention should be obtained from the City Administrator.
- (c) If, in the opinion of the City Administrator, a personnel complaint or disciplinary action maintained beyond the required retention period is no longer relevant, all records of such matter may be destroyed in accordance with the established records retention schedule.