**SECTION:** **EMPLOYEE CONDUCT AND ETHICS**

**POLICY:** Confidential Information **EFFECTIVE DATE:** insert date adopted

**STATEMENT OF PURPOSE:**

The purpose of this policy is to protect confidential information acquired or generated through city operations and ensure employees understand their responsibilities regarding the handling, use, and disclosure of such information. This policy supports legal compliance, safeguards public trust, and maintains the integrity of city services.

**DEFINTIONS:**

1. Confidential Information: Any information that is not publicly available and is protected by law, regulation, or policy, including but not limited to:
2. Personnel records
3. Medical or financial data
4. Social Security numbers
5. Investigation or litigation records
6. Proprietary or sensitive city data
7. Information protected under attorney-client privilege
8. Need-to-Know Basis: Access to information granted only if necessary to perform assigned duties.
9. Disclosure: The act of making confidential information available to unauthorized individuals or entities, either intentionally or unintentionally.

**APPLICABILITY:**

This policy applies to all city employees, elected officials, contractors, volunteers, interns, and any individuals with authorized access to city information systems or records, regardless of employment status or department.

**POLICY:**

All individuals with access to confidential information must protect it from unauthorized access, use, or disclosure. Confidential information must only be accessed or shared on a need-to-know basis in the performance of official duties. Improper handling or disclosure of confidential information may result in disciplinary action, legal liability, or termination of employment or service.

**PROCEDURES:**

1. Access and Use
2. Employees must only access confidential information necessary for the performance of their job duties.
3. Confidential information must not be discussed in public areas, including hallways, elevators, or social settings.
4. Physical and electronic records containing confidential information must be always secured.
5. Storage and Transmission
6. Paper records containing confidential information must be stored in locked cabinets or secure areas.
7. Electronic data must be protected using passwords, encryption, and other security measures in accordance with IT policies.
8. Email or digital transmission of confidential information must comply with city-approved encryption and security protocols.
9. Disclosure Restrictions
10. Confidential information may not be disclosed to unauthorized individuals, including coworkers without a business need, family members, media representatives, or the public.
11. Requests for confidential information from external parties must be referred to the City Attorney’s Office or designated public records officer.
12. Training and Acknowledgment
13. All employees will receive training on confidentiality policies during onboarding and as required thereafter.
14. Employees may be required to sign a confidentiality agreement as a condition of employment or service.
15. Reporting and Violations
16. Suspected breaches or unauthorized disclosures of confidential information must be reported immediately to a supervisor, Human Resources, or the City Attorney’s Office.
17. The city will investigate all reports of confidentiality violations and take appropriate corrective or disciplinary action.
18. Separation from Employment
19. Upon termination or separation, employees must return all city-owned documents and materials containing confidential information.
20. Obligations to maintain confidentiality continue beyond the term of employment or service.