CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

SUBJECT	Number	Issue	Page
	90.64	2	1 of 8
PROTECTION OF SENSITIVE INFORMATION AND DATA	Effective Date May 5, 2017		

1. PURPOSE

1.1. To establish a policy to ensure the confidentiality and protection of *Sensitive Information* against unauthorized use; to establish procedures to control access to *Sensitive Information* so that it is only accessible by *Authorized Persons*; and to establish safeguards to ensure the appropriate use of *Sensitive Information* by *Authorized Persons*.

1.2. To define responsibility and procedures for granting *Authorized Persons* access to *Sensitive Information*.

1.3. To define processes by which access to *Sensitive Information* is administered and to develop control points in compliance with City policy.

2. SCOPE

2.1. This policy applies to all City employees in all City departments, including independent departments as authorized by the signing authorities below; and to City volunteers, contractors, vendors, and other individuals granted access to *Sensitive Information* under the City's control by the nature of their support or service functions.

2.2. This policy and procedures apply to all Sensitive Information created, owned, stored, managed or under the control of the City of San Diego, regardless of the media which contains the Sensitive Information, including but not limited to paper, microfilm, microfiche or any analog or digital format.

2.3. Nothing in this Administrative Regulation supersedes any stricter requirement(s) set by other authorities (i.e., local, state, and/or federal laws, rules or regulations), such as obtaining or retaining employment in a law enforcement agency; nor does this Administrative Regulation supersede any applicable, stricter rules, regulations or policies that affect access to or use of *Sensitive Information*. In such cases, the department head must ensure implementation or application of any such superseding rules, regulations or policies include adequately strong internal controls over *Sensitive Information*.

(Supersedes Administrative Regulation 90.64, Issue 1, effective July 1, 2009)

Authorized

(*Signature on File*)

CHIEF OPERATING OFFICER

3. DEFINITIONS

3.1. *Appointing Authority* - An unclassified, management-level position designated by the department head or higher who has the authority to grant permission for an employee or individual to be authorized for access to *Sensitive Information*.

3.2. *Authorized Person* - An employee or other individual who is granted permission to access or use *Sensitive Information* by an *Appointing Authority*, as approved by the *Information/Data Owner*, at the type and the *Level of Access* to the specific information required for the performance of his or her job duties.

3.3. *Authorization Acknowledgment Form* - The City's official form used to request and authorize an individual's access to or use of *Sensitive Information* (see Appendix). This form will be available on the City's Intranet site (CityNet) on the 'Forms' page.

3.4. *Information/Data Owner* - The department head or designee who is the primary recipient or manager of particular *Sensitive Information* or who has the responsibility to oversee the collection, maintenance or management of such information or data. There will only be one defined *Information/Data Owner* for any particular source of data; although other departments may collect and/or access the data. An *Information/Data Owner* may also be an *Appointing Authority*, as defined in Section 3.1 above.

3.5. *Level of Access* - The amount of *Sensitive Information* for which access is granted for any specific category or type of *Sensitive Information*, such as full access to all information related to a particular category or document, or limited access to only specific pieces of information (i.e., certain fields in a database) required for the performance of valid job duties.

3.6. *Personal Identifying Information* - Shall include information listed in California Penal Code Section 530.55(b), as amended (Sept. 2006), which reads, in pertinent part:

3.6.1. *Person* - A natural *Person*, living or deceased, firm, association, organization, partnership, business trust, company, corporation, limited liability company, or public entity, or any other legal entity.

3.6.2. *Personal Identifying Information* - Any name, address, telephone number, health insurance number, taxpayer identification number, school identification number, state or federal driver's license or identification number, social security number, professional or occupational number, mother's maiden name, demand deposit account number, savings account number, checking account number, PIN (personal identification number) or password, alien registration number, government passport number, date of birth, unique biometric data including fingerprint, facial scan identifiers, voiceprint, retina or iris image, or other unique physical representation, unique electronic data including information identification number assigned to the *Person*, address or routing code, telecommunication identifying

information or access device, information contained in a birth or death certificate, credit card number of an individual *Person*, or an equivalent form of identification.

3.7. For the purpose of this policy, *Sensitive Information* shall mean:

3.7.1. *Personal Identifying Information* (as defined above), also including debit card number of an individual *Person*, and where home/personal address and telephone number are included and work/office address and telephone number are excluded (i.e., the City Directory is not considered *Sensitive Information*); and

3.7.2. Any information that is possessed by the City of San Diego which is not subject to the California Public Records Act (refer to Administrative Regulation 95.20), and which may be used for other than the intended purpose of such information, to cause harm to or otherwise jeopardize the City of San Diego or any individual, or used in violation of any local, state or federal law (for example the Health Insurance Portability and Accountability Act of 1996 (HIPAA)).

3.8. *Sensitive Information Custodian* - The *Person* who manages the physical or computer-based access to *Sensitive Information*; for example an office manager or records manager who controls access to locked file rooms/cabinets, or a computer systems administrator who manages the creation of user accounts and passwords to provide specific access to particular data. A *Sensitive Information Custodian* may also be an *Information/Data Owner*, as defined in Section 3.4. above.

3.9. *Type of Access* - Refers to Read Only, Write/Create, Edit/Modify, and Delete.

4. POLICY

4.1. *Sensitive Information* shall be maintained in a confidential manner and access restricted to only employees or individuals properly authorized by his or her *Appointing Authority* and approved by the *Information/Data Owner*, based on verified business needs to have access to such information and/or in compliance with specific legal requirements.

4.2. Contractors and vendors or other non-City employees who are authorized to access or use *Sensitive Information*, shall be required to enter into agreements stating that the individuals specified for this access and their employing Contractor/Vendor agree to be contractually bound by the terms and conditions of this policy, including personal liability, as part of their contract or agreement prior to being granted access to *Sensitive Information*.

4.3. Authorization to access or use *Sensitive Information* shall be based on a functional role (job duties) and not linked directly with a specific individual, such that when an *Authorized Person's* job duties no longer require access to or use of *Sensitive Information*, the ability to access or use such information shall be revoked. At no time shall a contractor's or vendor's access to *Sensitive Information* extend beyond the termination of the authorizing

contract, and such access shall be revoked as soon as the duties requiring access or use have ended, regardless of the end date of the contract.

4.4. The *Information/Data Owner* shall specify the type and the *Level of Access* that should be assigned to various functional roles that require access to the *Sensitive Information* based on an employee's or individual's job requirements.

4.5. *Authorized Persons* shall access or use *Sensitive Information* only for its intended purpose for which it was obtained and maintained by the City of San Diego. An employee or individual authorized to access or use *Sensitive Information* shall sign an *Authorization Acknowledgement Form* stating he or she has read, understands, and agrees to abide by this policy.

4.6. As a standard IT security measure, *Authorized Persons* shall not share their User ID and/or password with anyone else, and shall not have their User ID and/or password written down in any unsecured location (e.g., anywhere around their work location). "Generic" User IDs shall not be used for system access to *Sensitive Information*; each *Authorized Person* must use an assigned, unique User ID that is directly linked with the user's name. As a standard physical security measure, *Authorized Person*s shall not share their building or facility access key card or key(s) with anyone else, nor shall they allow access into secured areas by unauthorized *Persons*.

4.7. Violation of this policy, either by unauthorized *Persons* accessing or attempting to access *Sensitive Information*, or by *Authorized Persons* accessing or using *Sensitive Information* for other than its intended purpose or beyond the scope of their duties, may result in disciplinary action, up to and including termination of employment, and also subject the violating individual(s) to personal liability without the option of City legal defense. In the case of contractors or vendors, violation of this policy will be considered a breach of contract and appropriate actions taken on that basis. If deemed necessary, information regarding employee, volunteer, contractor or vendor violation of this policy may be referred to the appropriate agency for any civil and/or criminal action, as applicable.

4.8. Appointing Authorities shall review the list of their employees, contractors or other individuals who they have designated as *Authorized Persons* with access to *Sensitive Information*, at least semi-annually, to ensure continued authorization is warranted and to update (add, delete or modify) the authorization list appropriately.

4.9. *Information/Data Owners* shall verify and document semi-annually that the Appointing Authorities performed a thorough review of authorized users in compliance with this policy (Section 4.8.), by comparing the *Appointing Authority's* report with a list of individuals currently authorized to access the *Sensitive Information* over which the Information/Data Owner has control and authority. For internal control purposes, to maintain segregation of duties, this verification must be performed by someone other than the *Appointing Authority* who submitted the semi-annual review of *Authorized Persons*. All discrepancies shall be reported back to the impacted *Appointing Authority* for

appropriate corrective action. *Information/Data Owners* shall retain records of such reviews and actions for the period of time set within the citywide or departmental Records Retention Schedule as approved by the City Clerk.

4.10. *Sensitive Information* stored in City computer systems shall be secured and maintained in accordance with applicable provisions of the Information Security Guidelines and Standards, as amended.

4.11. *Sensitive Information* stored in paper or other non-digital formats shall have appropriate physical security, and access to such information shall also comply with Administrative Regulation 95.10 for validating the identity of the individual requesting authorized access.

4.12. Upon the discovery of any breach of the protection of *Sensitive Information* through the accidental, inadvertent or purposeful release of such information to any unauthorized *Persons*, the *Person* discovering such breach should immediately notify the *Information/Data Owner* or their *Appointing Authority*, and, if the information was stored on City computer systems, also notify the Chief Information Security Officer in the Department of Information Technology.

4.12.1. Depending on the nature and scope of such breach and release of information, additional notifications must comply with applicable state and federal regulations.

4.12.2. The Information/Data Owner, in coordination with the Chief Information Security Officer from the Department of Information Technology (if applicable), should immediately take whatever steps are deemed necessary to stop any further breach of the protected information and to minimize any potential or actual losses or damages to the City of San Diego.

5. RESPONSIBILITY

5.1. Supervisor

5.1.1. When an employee's, volunteer's or contractor's job duties require access to or use of *Sensitive Information*, the immediate supervisor will complete an Authorization Acknowledgment Form. In addition, the supervisor must ensure that the proper system access/account request form and process is followed for the specific computer system where the *Authorized Person* needs access, specifying the nature of the job duties and the level and *Type of Access* or use requested. The supervisor will ensure the accuracy and completeness of information on the forms. After obtaining the employee's signature, the acknowledgement and request forms will be routed to the *Appointing Authority* for approval. Likewise, when an employee's, volunteer's or contractor's job duties change such that access to or use of *Sensitive Information* is no longer needed, the immediate supervisor will notify both the

Appointing Authority and the *Information/Data Owner*, as soon as possible (no more than five (5) business days).

5.2. *Authorized Person* (employee, volunteer, contractor, vendor or other individual being authorized for access).

5.2.1. Any *Person* being given access to *Sensitive Information* must sign the *Authorization Acknowledgement Form* stating he or she has read, understands, and agrees to comply with this policy for access or use and protection of such information. A copy of the final, approved form shall be kept in the employee's departmental personnel file, as the *Appointing Authority's* record; or for volunteers, on file with the department where assigned; or for a contractor, on file with the contract manager.

5.3. Department *Appointing Authority*

5.3.1. The Department *Appointing Authority* having management control over the employee, volunteer, contractor Vendor or other individual seeking authorization to access *Sensitive Information*, shall review the Authorization Acknowledgement and system access/account request forms for appropriateness of the job functions for the type and *Level of Access* requested while considering appropriate segregation of duties, and ensure the forms are signed by both the individual and supervisor.

5.3.2. The Department *Appointing Authority* will sign either approval or denial of the request, providing the reasons for any denial, and route the approved request form to the appropriate *Information/Data Owner*(s), or route a denied form back to the supervisor. Appointing Authorities shall maintain a copy of all authorization forms they approve, including those for non-City employees (i.e., volunteers and contractors). Any changes reported in the job duties of *Authorized Persons* which require a change in the access to or use of *Sensitive Information* must be immediately communicated to the *Information/Data Owner* to initiate the appropriate change in access. The semi-annual reviews should take place in May and November each year. The *Appointing Authority* will submit documentation of each review to the *Information/Data Owner* and these records will be retained by the department for the period of time set by the citywide or departmental Records Retention Schedule as approved by the City Clerk.

5.4. Information/Data Owner (owner of the information, regardless of its format or mechanism of access, [i.e., computerized system, hard copy file, etc.])

5.4.1. The Information/Data Owner for each different source of *Sensitive Information* covered by an approved access request form will review each request to ensure the type and *Level of Access* requested is appropriate for the job functions of the individual seeking access. Upon confirmation of the business need to have access

to *Sensitive Information*, the Information/Data Owner will sign approval to grant access, and may modify the type or *Level of Access* granted, as he or she deems necessary and appropriate, in consultation with the requesting *Appointing Authority*. The Information/Data Owner will initiate any further actions necessary to grant access to the *Authorized Person* (such as any computer system access processes). *Information/Data Owners* will maintain a list of individuals currently authorized access to their *Sensitive Information* and provide such list to the appropriate *Appointing Authority* for semi-annual review at the end of April and October each year

5.5. *Sensitive Information Custodian* (Administrator of the format and/or mechanism of access [i.e., computerized system or hard copy file] for the given information)

5.5.1. The *Authorized Person's* access to the identified *Sensitive Information* will be set up following the established procedures either in the IT Security Guidelines and Standards for access to electronic or digital data or following departmental internal controls for paper or physical records, based on the nature (media/format) of the *Sensitive Information*.

5.6. Department of Information Technology

5.6.1. Annually review this policy for any necessary updates or revisions, taking into account changes in City organization and IT systems. Maintain the list of *Information/Data Owner*s and update it annually. Maintain the necessary correlation between this policy and other IT security policies and/or regulations. Ensure City third-party vendors who have access to this data comply with this and other IT security policies. The Department of Information Technology is also responsible for ensuring that the requirements of this policy are communicated to all employees at least annually, using citywide and/or departmental training or communication channels.

5.7. Purchasing & Contracting Department

5.7.1. Ensure that this policy is included as an Addendum to or within the Terms and Conditions of signed contracts or agreements, for all contracts and/or agreements that include a contractor's or vendor's need to access or use the City's *Sensitive Information*.

SUBJECT	Number	Issue	Page
	90.64	2	8 of 8
PROTECTION OF SENSITIVE INFORMATION AND DATA	Effective Date May 5, 2017		

APPENDIX

Legal References

Civil Service Rules and City Personnel Manual
Civil Service Rules, Definitions (p.l), "Appointing Authority"
Civil Service Rule XI, "Resignation, Removal, Suspension, Reduction in Compensation, Demotion"
Personnel Manual, Index Code A-3, "Improper Use of City Resources"
Personnel Manual, Index Code G-1, "Code of Ethics and Conduct"
Administrative Regulation 45.50 - Private Use of City Labor, Materials, Equipment and Supplies Prohibited
Administrative Regulation 90.63 - Information Security Policy
Administrative Regulation 95.10 - Identification of City Employees and Controlled Access to City Facilities
Administrative Regulation 95.20 - Public Records Act Requests and Civil Subpoenas; Procedures for Furnishing Documents and Recovering Costs
Administrative Regulation 95.60 - Conflict of Interest and Employee Conduct
IT Security Guidelines and Standards
Employee Performance Plans, Ethics and Integrity Section
Applicable California State Laws
Applicable Federal Laws

Forms Involved

Form DoIT-010A, "*Sensitive Information* Authorization Acknowledgement-City Employees"
Form DoIT-010B, "*Sensitive Information* Authorization Acknowledgement-City Volunteers"
Form DoIT-010C, "*Sensitive Information* Authorization Acknowledgement-City Contractors/Vendors"

Subject Index

Sensitive Information
Sensitive Data Information Security
Protection of *Sensitive Information*

Distribution

All Departments (Mayoral and Non-Mayoral)

Administering Department

Department of Information Technology

CITY OF SAN DIEGO

Sensitive Information Authorization Acknowledgement Form - City Employees

Authorized Person (City Employee requesting authorized access to Sensitive Information):

Name (Printed)	*Job Classification*	*Network (AD) Login/User ID*
Department / Division		
Mail Station	*Office Phone*	*Office FAX*
Supervisor's Name (Printed)	*Supervisors Phone*	

Policy Summary (pertinent excerpts from Administrative Regulation 90.64):

4.1. Sensitive Information shall be maintained in a confidential manner and access restricted to only employees or individuals properly authorized by his or her Appointing Authority and approved by the Information/Data Owner, based on verified business needs to have access to such information and/or in compliance with specific legal requirements.

4.3. Authorization to access or use Sensitive Information shall be based on a functional role (job duties) and not linked directly with a specific individual, such that when an authorized person's job duties no longer require access to or use of Sensitive Information, the ability to access or use such information shall be revoked. [...]

4.5. Authorized Persons shall access or use Sensitive Information only for its intended purpose for which it was obtained and maintained by the City of San Diego. An employee or individual authorized to access or use Sensitive Information shall sign an Authorization Acknowledgement Form stating he or she has read, understands, and agrees to abide by this policy.

4.7. Violation of this policy, either by unauthorized persons accessing or attempting to access Sensitive Information, or by Authorized Persons accessing or using Sensitive Information for other than its intended purpose or beyond the scope of their duties, may result in disciplinary action, up to and including termination of employment, and also subject the violating individual(s) to personal liability without the option of City legal defense. In the case of contractors or vendors, violation of this policy will be considered a breach of contract and appropriate actions taken on that basis. If deemed necessary, information regarding employee, volunteer, contractor or vendor violation of this policy may be referred to the appropriate agency for any civil and/or criminal action, as applicable.

Acknowledgement

By signing below, the above employee acknowledges the he or she has been provided a full copy of A.R. 90.64 ("Protection of Sensitive Information and Data"), which has been discussed with his or her supervisor, and further acknowledges that he or she has read, understands, and agrees to comply with the provisions of the policy. Employee understands that this form will be kept as part of his or her permanent employee file, and that he or she may receive a copy, if requested. The supervisor acknowledges that he or she has discussed the policy with the above employee and understands the supervisor's obligations regarding employee's access to Sensitive Information under this policy.

_____ _____

Employee's Signature Date Signed

_____ _____

Supervisor's Signature Date Signed

CITY OF SAN DIEGO

Sensitive Information Authorization Acknowledgement Form- City Volunteers

Authorized Person (City Volunteer requesting authorized access to Sensitive Information):

Name (Printed)	*Volunteer Assignment*	*Network (AD} Login/User ID*
City Department / Division (where assigned as volunteer)		
Work Location		*Contact Phone*
City Supervisor's Name (Printed)	*City Supervisor's Phone*	*City Supervisor's Mail Station*

Policy Summary (pertinent excerpts from Administrative Regulation 90.64):

4.1. Sensitive Information shall be maintained in a confidential manner and access restricted to only employees or individuals properly authorized by his or her Appointing Authority and approved by the Information/Data Owner, based on verified business needs to have access to such information and/or in compliance with specific legal requirements.

4.3. Authorization to access or use Sensitive Information shall be based on a functional role Job duties) and not linked directly with a specific individual, such that when an authorized person's job duties no longer require access to or use of Sensitive Information, the ability to access or use such information shall be revoked. At no time shall a contractor's or vendor's access to Sensitive Information extend beyond the termination of the authorizing contract, and such access shall be revoked as soon as the duties requiring access or use have ended, regardless of the end date of the contract.

4.5. Authorized Persons shall access or use Sensitive Information only for its intended purpose for which it was obtained and maintained by the City of San Diego. An employee or individual authorized to access or use Sensitive Information shall sign an Authorization Acknowledgement Form stating he or she has read, understands, and agrees to abide by this policy.

4.7. Violation of this policy, either by unauthorized persons accessing or attempting to access Sensitive Information, or by Authorized Persons accessing or using Sensitive Information for other than its intended purpose or beyond the scope of their duties, may result in disciplinary action, up to and including termination of employment, and also subject the violating individual(s) to personal liability without the option of City legal defense. In the case of contractors or vendors, violation of this policy will be considered a breach of contract and appropriate actions taken on that basis. If deemed necessary, information regarding employee, volunteer, contractor or vendor violation of this policy may be referred to the appropriate agency for any civil and/or criminal action, as applicable.

Acknowledgement

By signing below, the above City Volunteer acknowledges the he or she has been provided a full copy of A.R. 90.64 ("Protection of Sensitive Information and Data"), which has been discussed with the City Supervisor, and further acknowledges that he or she has read, understands, and agrees to comply with the provisions of the policy. City Volunteer understands that this form will be kept on file with the City Department, and that he or she may receive a copy, if requested. The City Supervisor acknowledges that he or she has discussed the policy with the above volunteer and understands the supervisor's obligations regarding the volunteer's access to Sensitive Information under this policy.

_____ _____

Volunteer's Signature Date Signed

_____ _____

City Supervisor's Signature Date Signed

CITY OF SAN DIEGO

Sensitive Information Authorization Acknowledgement Form- City Contractors/Vendors

Authorized Person (City Contractor/Vendor requesting authorized access to Sensitive Information):

Name (Printed)	*eMail Address*	*Network (AD) Login/User ID*
Company/Organization		*Contractor/Vendor Office Phone*
City Department (managing contract)		*Contractor/Vendor Office FAX*
City Contract Manager's Name (Printed)	*City Contract Manager'8 Phone*	*City Contract Manager's Mail Sta.*

Policy Summary (pertinent excerpts from City Administrative Regulation 90.64):

4.1. Sensitive Information shall be maintained in a confidential manner and access restricted to only employees or individuals properly authorized by his or her Appointing Authority and approved by the Information/Data Owner, based on verified business needs to have access to such information and/or in compliance with specific legal requirements.

4.3. Authorization to access or use Sensitive Information shall be based on a functional role (job duties) and not linked directly with a specific individual, such that when an authorized person's job duties no longer require access to or use of Sensitive Information, the ability to access or use such information shall be revoked. At no time shall a contractor's or vendor's access to Sensitive Information extend beyond the termination of the authorizing contract, and such access shall be revoked as soon as the duties requiring access or use have ended, regardless of the end date of the contract.

4.5. Authorized Persons shall access or use Sensitive Information only for its intended purpose for which it was obtained and maintained by the City of San Diego. An employee or individual authorized to access or use Sensitive Information shall sign an Authorization Acknowledgement Form stating he or she has read, understands, and agrees to abide by this policy.

4.7. Violation of this policy, either by unauthorized persons accessing or attempting to access Sensitive Information, or by Authorized Persons accessing or using Sensitive Information for other than its intended purpose or beyond the scope of their duties, may result in disciplinary action, up to and including termination of employment, and also subject the violating individual(s) to personal liability without the option of City legal defense. In the case of contractors or vendors, violation of this policy will be considered a breach of contract and appropriate actions taken on that basis. If deemed necessary, information regarding employee, volunteer, contractor or vendor violation of this policy may be referred to the appropriate agency for any civil and/or criminal action, as applicable.

Acknowledgement

By signing below, the above City Contractor/Vendor acknowledges the he or she understands that the Terms and Conditions of the underlying City Contract contain the provisions of the full policy stated above, and he or she agrees to comply with such contract provisions. City Contractor/Vendor understands that this form will be kept on file with the underlying contract documents in the City Purchasing & Contracting Department, and that he or she may receive a copy, if requested. The City Contract Manager acknowledges that he or she has discussed the contract Terms and Conditions related to this policy with the above Contractor/Vendor and understands the supervisor's obligations regarding the Contractor's/Vendor's access to the City's Sensitive Information under this policy.

_____ _____

Contractor's/Vendor's Signature Date Signed

_____ _____

City Contract Manager's Signature Date Signed