CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

SUBJECT	Number	Issue	Page
	90.63	2	1 of 12
INFORMATION SECURITY POLICY	Effective Date May 5, 2017		

1. PURPOSE

1.1. To ensure *City Information* is accurate, relevant, properly protected, and handled consistent with City policies and *Standards*.

1.2. To establish *Information Security Policies* and procedures for protection of *City Information* and the use of City *Computer Equipment*, Network Services, and *Electronic Mail* (*Email*) and non-City or personal *Computer Equipment* that may be used to access City *Computer Equipment*, *Computer Systems* or *Network Services* by any person or affiliate that is subject to this Administrative Regulation.

1.3. To establish a procedure for approving and notifying employees, and other individuals and entities subject to this Administrative Regulation, about *Information Security Standards and Guidelines* that will provide specific guidance and criteria in securing and using City *Computer Equipment*, *Network Services*, and *Email*.

1.4. To establish the basis for an Identity Theft Prevention Program, to ensure the security and safety of both employee and citizen/customer personal information.

2. SCOPE

2.1. This regulation applies to all City employees, contractors, volunteers, and other affiliates, sometimes collectively referred to as "Individuals," using some or all of the City of San Diego's *Computer Systems*, Computer Equipment, *Network Services* or Email system.

2.2. This regulation applies to the use of City *Computer Equipment* or *Network Services* and to non-City or personal computer equipment that may be used to access City *Computer Systems* or *Network Services* by any Individual subject to this Administrative Regulation.

3. DEFINITIONS

3.1. *Breach* - Means unauthorized access to the City's Computer Equipment, *Computer Systems*, Email, or *Network Services* was, or is reasonably believed to have been, acquired by an unauthorized person.

(Supersedes Administrative Regulation 90.63, Issue 1, effective June 30, 2011)

Authorized

(*Signature on File*)

CHIEF OPERATING OFFICER

3.2. *City Information* - Includes information relating to the conduct of the public's business which is prepared, owned, used or retained by any City department or Individual regardless of physical form or characteristics.

3.3. *Computer Equipment* - Includes computer hardware and peripherals, including monitor, mouse, keyboard, and printers, tablets, portable or laptop computers, smart phones and similar communication equipment owned, operated or maintained by the City or an information technology (IT) service provider under contract with the City.

3.4. *Computer Systems* - Includes a network system, interconnected *computer equipment* (e.g., servers and storage devices), software package, or other IT resources.

3.5. *Email (Electronic Mail)* - A method of composing, storing, sending, and receiving (electronic transfer of information) electronic messages, memoranda, and attached documents from a sender to one or more recipients via a telecommunications network.

3.6. *Guidelines* - Recommended actions and/or industry best practices that should be used regarding security practices for ensuring compliance with policies and *standards*.

3.7. *Information Security* - An attribute of information systems which includes specific policy-based mechanisms, practices, procedures, and assurances for protecting the confidentiality and integrity of information, the availability and functionality of critical services, and the privacy of individuals.

3.8. *Information Security Standards and Guidelines* - Means the *standards* and *guidelines* developed by the Department of IT and approved by the appropriate IT governance body which govern operation of City *Computer Systems*, *Computer Equipment*, *Email*, and *Network Services*.

3.9. *Information Security Policies* - Organizational rules and practices that regulate how an organization manages, protects, and uses its information system assets and data.

3.10. *Internet* - A publicly accessible network connecting *Computer Systems* throughout the world using the standard *Internet* Protocol (IP). In addition to providing capability for *Email*, other *Internet* applications include, but are not limited to, news groups, data processing & storage services, data transfer services, *Email*, cloud services, and the world-wide web ("WWW" or "Web").

3.11. *Network Services* - Communication networks, including the underlying infrastructure of routers, switches, wireless access points, and communications media for hard-wired or wireless transmission of data across the network. Local Area Networks (LANs), Wide Area Networks (WANs), the *Internet*, and wireless networks are examples of *Network Services*.

3.12. *Standards* - Indicates how and what kind of software, hardware, databases, and business practices should be implemented, used, and maintained to meet security and operational objectives.

3.13. *System Managers or System Administrators* - Individuals who support the operations and integrity of City *Computer Systems* and their use. Their activities might include system installation, configuration, integration, maintenance, security management, and problem analysis and recovery. By the nature of their duties, they have administrative-level access to *Computer Systems*, including operating systems, applications, databases, software utilities, and computer hardware, not accessible by standard *Users.*

3.14. *User* - Any individual who has been granted privileges and access to City *Computer Equipment*, *Network Services*, applications, resources, or information. *User* is also any person who is identified in Sections 2.1. and 2.2. above.

3.15. *User ID or User Account* - The unique account identifier that is assigned to a *User* of the City's *Computer Equipment*, *Computer Systems*, and *Network Services*.

4. POLICY

4.1. General

4.1.1. Guidance, direction, and authority for *Information Security* activities are centralized for the City under the Department of Information Technology ("Dept. of IT"), Chief *Information Security* Officer (CISO).

a. The Dept. of IT will provide direction and expertise to ensure the City's information is protected. This responsibility includes consideration of the confidentiality, integrity and availability of both information and *Computer Systems* that manage information. The Dept. of IT will act as a liaison for all *Information Security* matters with all City departments and IT service providers, and must be the focal point for all *Information Security* activities throughout the City. The Dept. of IT will participate in vendor product evaluations and in-house system development projects, assist with implementing security controls, investigate *Information Security Breach*es and perform other activities which are necessary to assure a secure information handling environment.

b. The Dept. of IT has the authority to provide exceptions to specific provisions of this policy based upon unique business requirements and other considerations. Departments will promptly notify the Dept. of IT in the event an exception is being requested for the security requirements of their respective *Computer Systems.* All exception requests and resulting actions must be fully documented and will be retained by the Dept. of IT.

4.1.2. All computer files developed, created or enhanced within the scope and course of City employment, or a City third-party contractual relationship, are the property of the City of San Diego, regardless of their physical location or the form in which they are maintained. These include, but are not limited to, computer data files, documents, databases, spreadsheets, calendar entries, appointments, tasks, and notes which reside on any City *Computer Systems* or *Computer Equipment*, or the *computer equipment* of a contractor performing work for or on behalf of the City.

a. The City reserves the right to access and disclose as required or permitted by law, and as defined in the approved *Information Security Standards and Guidelines*, all messages and other electronic data sent over its *Email* systems or stored in computer files on City *Computer Equipment*. City-related computer files stored on non-City or personal computers must be provided upon the City's request in City standard formats.

b. It is the responsibility of the Department Head or designee to ensure access to City *Computer Systems* is terminated and all computer files are properly handled by the City when an employee leaves City employment, pursuant to applicable City regulations, policies, and procedures.

c. All inventions, improvements, developments, or other works and any related copyrights, trademarks, patents or other intellectual property rights which are in any way related to City business or activities and which are created, developed, enhanced, or are derived, by one or more City employees during the employee's employment and compensated working hours, or using City *Computer Equipment*, or otherwise developed within the scope of an employee's employment, are the exclusive intellectual property rights of the City of San Diego and the City shall own all rights in such intellectual property, including any applicable copyright, patent, trademark, or other intellectual property rights.

4.1.3. Access to information available through the City's *Network Services* or from the City's *Computer Systems* is controlled by Dept. of IT approved access control criteria and *Information Security Standards and Guidelines*, which are to be maintained and reviewed at least annually, including updates, as necessary.

4.1.4. Authorized access to City *Computer Systems* and *Network Services* shall be at the minimum level required for the Individual to perform and complete their assigned duties, and not at a level that allows access to information beyond the scope of that Individual's assigned duties.

4.1.5. Each *Computer System* or *Network Services User ID* must uniquely identify only one *User*. Generic, shared, or group *User IDs* are not permitted. Any unique *User ID* shall not be duplicated across multiple *user* authentication directories,

so that there is always only one source *User* directory for authenticating any *User ID* for access to City *Computer Systems* or *Network Services*. Network security groups may be used to combine *Users* access rights. Approved group *Email* accounts may be shared by multiple *Users* who each have unique *User IDs*.

a. Any Department that requires Individuals to share a single *Computer System*, such as a desktop PC used for customer service, must ensure compliance with the shared-use workstation requirements of the *Information Security Standards and Guidelines.*

4.1.6. The initial login password issued to a *User* must be valid only for that *User*'s first online session. At the time of initial login, the system must force the *User* to create another password before any other work can be done on the system. Passwords must meet the current criteria set in the *Information Security Standards and Guidelines.*

4.1.7. *Network Services* are an essential component of the City's information resources. No device may be connected to the City's *Computer Systems*, data network or voice network unless it has been specifically approved by the Department of Information Technology (IT) pursuant to *Information Security Standards and Guidelines* adopted in accordance with this policy. This section excludes portable data storage devices/media, such as USB drives, being connected to an existing City computer, as long as proper security measures are taken with those devices to prevent and avoid infection by malicious software (i.e., virus or Trojan).

4.1.8. All servers, network equipment or telecommunications equipment used for the production support of City business operations must utilize uninterruptible power supply (UPS) and surge protection. Devices deemed critical to City business operations should be on dual power grids or on emergency power generators to protect against power outages.

4.1.9. Portable storage devices should only be used for temporary storage of data. Any City data or records created on portable storage devices, such as CDs or USB drives, are to be treated according to Section 4.1.2. above. The content should be made accessible in a standard format and should comply with the *Information Security Standards and Guidelines*. City records stored on portable storage devices must be retained in accordance with applicable laws, rules, regulations, and policies pertaining to the management and retention of City records.

4.1.10. Misrepresenting, obscuring, suppressing, or replacing a *User's* identity on an electronic communications system is forbidden. The *User* name, *Electronic Mail*

address, and related information used for login/access and included with messages or online postings must reflect the actual originator of the messages or postings.

4.1.11. *User*s shall not download or store software from the *Internet* on City *Computer Equipment* which has not been properly licensed to the City or in which the City does not have a legal right to possess or use. *Users* shall not install unauthorized or unlicensed software programs on City *Computer Equipment*. Any authorization must be obtained in advance from the Department of IT.

4.1.12. An *Information Security* Committee or its successor, as defined and chartered through the City's IT governance structure, will meet periodically to review the current status of the City's *Information Security*, review and monitor security incidents within the City, approve and periodically review *Information Security* projects, and provide semi-annual reports related to these activities to the Dept. of IT.

a. The *Information Security* Committee will review this policy and the related *Information Security Standards and Guidelines* annually during the first quarter of each fiscal year, making recommendations for any updates to the Dept. of IT. The Dept. of IT will forward any recommended updates to the City executive management team for approval.

4.2. Departmental Management Policy

4.2.1. Department Directors are ultimately responsible for departmental compliance with the provisions of this policy and other *information security* and acceptable use policies.

4.2.2. Senior management will lead by example by ensuring *Information Security* is given a high priority in all current and future business activities and initiatives.

4.2.3. Management must provide all *Users* within their department with sufficient training to allow them to understand their personal responsibilities to properly protect information resources, including tracking of the dates and names of employees trained. *Information Security* training materials will be created, maintained, and made available by the Dept. of IT. Such training should occur within the first 90 days of employment, and then refresher training should occur annually for all employees.

4.2.4. Management must allocate sufficient on-the-job time for *Users* to acquaint themselves with *Information Security Policies*, separately from the formal training required in Section 5.3 above, including the *Information Security Standards and Guidelines* with related procedures on prohibited activities and

appropriate ways to report security threats. Management must notify *Users* of specific actions that constitute security violations and that such violations will be logged.

4.2.5. Each department will designate an *Information Security* Liaison (ISL) to be the primary point of contact responsible for department compliance with the City's *Information Security Policies* and coordination with the Dept. of IT. The *Information Security* Liaison should be a senior IT staff member or unclassified manager. The City's Chief *Information Security* Officer will manage the ISL program and provide information and training pertinent to the position to assist in protecting City IT assets.

4.2.6. Each department will review their own security practices at least annually for conformance with this policy and compliance with the *Information Security Standards and Guidelines*.

4.2.7. All department and City *Computer Systems* privileges must be promptly terminated at the time a *User* leaves City employment or ceases to provide services to or receive services from the department or the City. Such termination of access to City *Computer Systems* includes revocation of the assigned *User ID* and must occur as soon as possible and, in any case, no more than three (3) business days, after access is no longer required. All files held in the *User's* home directory, as applicable, will be held for 90 days for their supervisor or designee to review and will then be deleted. All City records shall be retained in accordance with the department's approved Records Disposition Schedule or the Citywide General Records Disposition Schedule.

4.2.8. Records reflecting the *Computer Systems* on which *Users* have accounts must be kept up-to-date and reviewed periodically, at least annually, by the respective Department Head or designee, so *Computer Systems* access privileges may be expeditiously revoked on short notice, if the need arises.

4.2.9. To provide evidence for investigation, prosecution or disciplinary actions, relevant *Computer Systems* information should be immediately captured and preserved whenever it is suspected that a computer *Breach*, crime or abuse has taken place. The relevant information must be securely stored offline until such time as legal counsel determines the City will no longer need the information. The information to be immediately collected shall include the current system status and backup copies of all potentially involved files. The *Information Security* Liaison or *User* who discovers the suspected *Breach*, crime or abuse should report such to the Dept. of IT, Chief *Information Security* Officer who will take action to preserve the relevant information.

4.2.10. To ensure a quick, effective, and orderly response to *information security* incidents, the *Information Security* Committee will identify a "Cyber Security Incident Response Team" (CSIRT) comprised of IT staff to handle the reporting of and response to *information security* incidents. The reporting of incidents will be done according to the *Information Security Standards and Guidelines* .

4.2.11. All known vulnerabilities of the City's *Computer Systems*, in addition to suspected or known violations, must be communicated in an expeditious and confidential manner to the Dept. of IT, the Chief *Information Security* Officer, the IT Service Provider, and any others designated by the Dept. of IT.

4.2.12. Except as specifically provided for in this policy, other *Information Security Policies* and procedures or otherwise provided by law, reporting *information security* violations, problems or vulnerabilities to any person outside the City, except to an appropriate government or law enforcement agency, without the prior written approval of the Dept. of IT, is strictly prohibited.

4.2.13. Criticality levels will be assigned to each business application to reflect the potential impacts resulting from a *Breach*, data corruption or denial of service. No less than once every two years, the Dept. of IT will conduct a rating survey to inventory and assign criticality levels to City applications. Each Department Director or their designee will assign criticality levels and data elements based on criteria established by the *Information Security* Committee. The Dept. of IT will maintain a master list of all inventoried applications and assigned ratings.

4.3. *User* Policy

4.3.1. *Users* must be responsible in their use of City *Computer Equipment*, and *Network Services*. Any action that may cause interference with City *Computer Systems* exposes the City's *Computer Systems* to risk or adversely impacts the work of others in using these *Computer Systems* is prohibited.

4.3.2. Employees may be disciplined in accordance with standard City procedures for improperly using or knowingly allowing the improper use of the City's *Computer Equipment*, *Network Services* or *Email* system as stated in this regulation. Abuse of the City's *Computer Systems* may result in disciplinary action, up to and including termination and criminal prosecution if deemed appropriate.

4.3.3. Employees should cooperate fully with all investigations, regarding the abuse of the City's *Network Services*, *Computer Equipment*, *Computer Systems*, and the *Internet*.

4.3.4. Every end *User* must have a single unique *User ID* and a personal password which must be kept confidential and not shared with anyone else. This *User ID* and

password will be required for access to all multi-*user Computer Equipment* and *Network Services*. *User* passwords must comply with the *Information Security Standards and Guidelines*.

4.3.5. *Users* accessing City *Computer Systems* are prohibited from gaining unauthorized access to any other non-City *computer systems* or in any way damaging, altering or disrupting the operations of those systems. *Users* are also prohibited from capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism which could permit unauthorized access.

4.3.6. Employees who use City *Computer Systems*, *Computer Equipment*, *Network Services*, or the City's *Email* shall sign an *Information Security* Policy Acknowledgement Form which states that the employee agrees to comply with the terms of this Administrative Regulation.

4.4. System Manager/Administrator Policy

4.4.1. Every multi-*user* system must include sufficient automated tools to assist *System Managers* in verifying the security status of the *Computer Equipment* and *Computer Systems*. These tools must include mechanisms for automated notifications to be sent to *System Managers* and for the correction of security problems.

4.4.2. Whenever a City *Computer System* has been *Breached* by an unauthorized party, or there is a reasonable suspicion of a *Breach* or other system compromise, *System Managers* must immediately change the password on the involved system and any other systems at risk from the *Breach*ed account. Under either of these circumstances, all recent changes to *User* and system privileges must be reviewed for unauthorized modifications.

4.4.3. Production application systems which access financial or sensitive information must generate logs that show every addition, modification, and deletion to such information.

4.4.4. Mechanisms used to detect and record significant computer security events must be resistant to attacks. These attacks include attempts to deactivate, modify, or delete the logging software or the logs themselves.

4.4.5. All *Computer Systems* and application logs must be maintained in an environment where they cannot readily be viewed by unauthorized persons. By definition, a person is unauthorized if he or she is not a member of the authorized network security group(s) which allow access to such logs.

4.4.6. Logs of computer security related events must provide sufficient data to support comprehensive audits of the effectiveness of, and compliance with, security measures. Logs containing computer security related events must be retained in accordance with the applicable department's Records Disposition Schedules or the Citywide General Records Disposition Schedule. During this period, the logs must be secured so that they cannot be modified, and so that they can be read only by authorized persons. These logs are important for error correction, forensic auditing, security *Breach* recovery, and related efforts.

4.4.7. To allow proper remedial action, *System Managers* must, on a daily basis, review records reflecting security relevant events on multi-*user* machines/systems.

4.4.8. When a person who is authorized as a System Manager or System Administrator ceases to perform those functions, then such person's access to City *Computer Systems*, *Computer Equipment*, *Network Services*, and applications must be immediately revoked and system-level passwords to which he or she had access must be changed as soon as possible and, in any case, no more than twenty-four (24) hours after such System Manager or System Administrator ceases to perform those functions. In addition, such person's physical access to City *Computer Systems*, *Computer Equipment*, and *Network Services* must be restricted or revoked immediately, as appropriate.

5. RESPONSIBILITY

5.1. Mayor

5.1.1. The Mayor will establish regulations and procedures regarding the security and safeguarding of City data, *Computer Equipment*, *Computer Systems*, and *Network Services*.

5.2. Chief Information Officer

5.2.1. The Chief Information Officer has the responsibility to provide *Guidelines*, strategic direction, oversight, and coordination of citywide *Computer Systems*.

5.3. Chief *Information Security* Officer

5.3.1. The Chief *Information Security* Officer or designee will direct and manage the planning and supervision of all *Information Security* services for the City, including those provided by vendors/providers.

5.4. Strategic Technology Advisory Committee (STAC)

5.4.1. The Strategic Technology Advisory Committee (STAC) or other IT governing

body as assigned by the City Chief Operating Officer is responsible for approving *Information Security Standards and Guidelines*.

5.5. *Information Security* Committee

5.5.1. The *Information Security* Committee or other IT governing body as assigned by the STAC is responsible for reviewing departments' initial requests for exemptions from the *Information Security Standards and Guidelines* and recommending modifications to the City's existing *Information Security Standards and Guidelines*, as necessary.

5.6. IT Services Provider(s)

5.6.1. The City's IT services provider(s) will be responsible for providing, operating, and maintaining the City's primary *Computer Systems*, and *Email* systems, *Network Services*, and *Internet* connectivity. The IT services provider is charged with the responsibility of protecting the City's *Network Services* and *Computer Systems* from intrusion from outside sources, including the management and maintenance of firewalls.

5.7. Department Directors

5.7.1. Department Directors or their designees are responsible for approving requests for *User IDs* and *User Account*s for *Email* and *Network Services*.

5.8. *Information Security* Liaison

5.8.1. The departmental *Information Security* Liaison is the primary point of contact responsible for department compliance with the City's *Information Security Policies*.

5.9. System Administrators and System Managers

5.9.1. *System Administrators* and *System Managers* are responsible for maintaining the security and integrity of City *Computer Systems* and *Network Services*, including duties related to creating, modifying, and deleting *User IDs* or *User Account*s, and for maintaining the confidentiality of data contained on those systems in compliance with the City's *Information Security Policies*.

5.10. IT Asset Manager

5.10.1. The department IT Asset Manager is responsible for maintaining an accurate, up-to-date inventory of all departmental IT assets, including computer hardware and software.

5.11. Supervisory Personnel

5.11.1. Supervisory Personnel are responsible for overseeing the employee's use of City *Computer Systems*, *Email* systems, and *Network Services*.

5.12. Every Individual is responsible for his/her actions and conduct in accessing or using the City's *Computer Systems*, *Network Services*, and *Email* Systems. Violation of the City's *Information Security Policies* or unauthorized or inappropriate use may result in disciplinary action.

APPENDIX

Legal References

San Diego Municipal Code, section 27.3564(b)
Administrative Regulation 45.50 - Private Use of City Labor, Equipment, Materials, and Supplies Prohibited
Administrative Regulation 90.20 - Office Telephones
Administrative Regulation 90.62 - Information and Communications Technology Acceptable Use
Administrative Regulation 90.64 - Protection of Sensitive Information and Data
Administrative Regulation 90.65 - Broadcast Email and Voice Mail

Forms Involved

Employee Acknowledgement of IT Security Policy Overview
Form IT-063 - Information Security Policy Acknowledgement

Subject Index

Computer Equipment, Security Computer Systems, Security
Electronic Mail, Security Email, Security
Internet, Security
Network Services, Security
Security – Information Technology

Distribution

All Departments (Mayoral and Non-Mayoral)

Administering Department

Department of IT

CITY OF SAN DIEGO

Information Security Policy Acknowledgement Form – City Employees

Policy Summary (pertinent excerpts from Administrative Regulation 90.63):

4.1.2. All computer files developed, created or enhanced within the scope and course of City employment, or a City third-party contractual relationship, are the property of the City of San Diego, regardless of their physical location or the form in which they are maintained. These include, but are not limited to, computer data files, documents, databases, spreadsheets, calendar entries, appointments, tasks, and notes which reside on any City Computer Systems or Computer Equipment, or the Computer Equipment of a contractor performing work for or on behalf of the City.

a. The City reserves the right to access and disclose as required or permitted by law, and as defined in the approved Information Security Standards and Guidelines, all messages and other electronic data sent over its Email systems or stored in computer files on City Computer Equipment. City-related computer files stored on non-City or personal computers must be provided upon the City's request in City standard formats.

4.1.4. Authorized access to City Computer Systems and Network Services shall be at the minimum level required for the Individual to perform and complete their assigned duties, and not at a level that allows access to information beyond the scope of that Individual's assigned duties.

4.1.5. Each Computer System or Network Services User ID must uniquely identify only one User. Generic, shared, or group User IDs are not permitted. [...] Network security groups may be used to combine Users access rights. Approved group Email accounts may be shared by multiple Users who each have unique User IDs.

4.3.1. Users must be responsible in their use of City Computer Equipment, and Network Services. Any action that may cause interference with City Computer Systems, exposes the City's Computer Systems to risk or adversely impacts the work of others in using these Computer Systems is prohibited.

4.3.2. Employees may be disciplined in accordance with standard City procedures for improperly using or knowingly allowing the improper use of the City's Computer Equipment, Network Services or Email system as stated in this regulation. Abuse of the City's Computer Systems may result in disciplinary action, up to and including termination and criminal prosecution if deemed appropriate.

4.3.4. Every end User must have a single unique User ID and a personal password which must be kept confidential and not shared with anyone else. This User ID and password will be required for access to all multi-user Computer Equipment and Network Services. User passwords must comply with the Information Security Standards and Guidelines.

4.3.5. Users accessing City Computer Systems are prohibited from gaining unauthorized access to any other non-City Computer Systems or in any way damaging, altering or disrupting the operations of those systems. Users are also prohibited from capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism which could permit unauthorized access.

Employee/Supervisor Acknowledgement

By signing below, the employee acknowledges that he or she has been advised of the City's policies related to Information Security as provided in Administrative Regulation 90.63 ("Information Security Policy"), which has been discussed with his or her supervisor, and further acknowledges that he or she 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 departmental employee file, and that he or she may receive a copy, if requested. The supervisor acknowledges that he or she has discussed the policy (A.R. 90.63) with the employee named below and understands the supervisor's obligations regarding Information Security under this policy.

_____
Employee's Name (Print Legibly)

_____ _____
Employee's Signature Date Signed

_____
Supervisor's Name (Print Legibly)

_____ _____
Supervisor's Signature Date Signed