

Acceptable Use Practice

1 Overview

The purpose of this practice is to establish acceptable and unacceptable use of electronic devices and network resources at the City of Santa Ana in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.

The City of Santa Ana provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This practice requires the users of information assets to comply with City policies and protects the City against damaging legal issues.

2 Scope

All employees, contractors, consultants, temporary and other workers at the City of Santa Ana, including all personnel affiliated with third parties must adhere to this practice. This practice applies to information assets owned or leased by the City, or to devices that connect to a City network or reside at a City site.

Information Services Operations Division must approve exceptions to this policy in advance.

3 Practice Statement

3.1 General Requirements

- 3.1.1 You are responsible for exercising good judgment regarding appropriate use of the City of Santa Ana resources in accordance with City policies, standards, and guidelines. The City resources may not be used for any unlawful or prohibited purpose.
- 3.1.2 For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, and network traffic. Devices that interfere with other devices or users on the City network will be disconnected. Information Security prohibits actively blocking authorized audit scans. Firewalls and other blocking technologies must permit access to the scan sources.

3.2 System Accounts

- 3.2.1 You are responsible for the security of data, accounts, and systems under your control. Keep passwords secure and do not share account or password information with anyone, including other personnel, family, or friends. Providing access to another individual, either deliberately or through failure

to secure its access, is a violation of this practice.

- 3.2.2 You must maintain system-level and user-level passwords in accordance with the City's Password Policy.
- 3.2.3 You must ensure through legal or technical means that proprietary information remains within the control of the City at all times. Conducting City business that results in the storage of proprietary information on personal or non- City controlled environments, including devices maintained by a third party with whom the City does not have a contractual agreement, is prohibited. This specifically prohibits the use of an e-mail account that is not provided by the City, or its customer and partners, for company business.

3.3 Computing Assets

- 3.3.1 You are responsible for ensuring the protection of assigned City assets that includes the use of computer cable locks and other security devices. Laptops left at the City overnight must be properly secured or placed in a locked drawer or cabinet. Promptly report any theft of City assets to Information Services or your local administrator.
- 3.3.2 All PCs, portable devices, laptops, and workstations must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.
- 3.3.3 Do not interfere with the City's device management or security system software, including, but not limited to antivirus.

3.4 Network Use

You are responsible for the security and appropriate use of the City network resources under your control. Using City resources for the following is strictly prohibited:

- 3.4.1 Causing a security breach to either the City or other network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorized; circumventing user authentication on any device; or analyzing network traffic.
- 3.4.2 Causing a disruption of service to either the City or other network resources, including, but not limited to, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes.
- 3.4.3 Introducing honeypots, honeynets, or similar technology on the City network.
- 3.4.4 Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software.

- 3.4.5 Exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws.
- 3.4.6 Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and keyloggers.
- 3.4.7 Port scanning or security scanning on a production network unless authorized in advance by Information Security.

3.5 Electronic Communications

The following are strictly prohibited:

- 3.5.1 Inappropriate use of communication vehicles and equipment, including, but not limited to, supporting illegal activities, and procuring or transmitting material that violates the City policies against harassment or the safeguarding of confidential or proprietary information.
- 3.5.2 Sending spam via e-mail, text messages, pages, instant messages, voice mail, or other forms of electronic communication.
- 3.5.3 Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.
- 3.5.4 Posting the same or similar non-business-related messages to large numbers of newsgroups (newsgroup spam).
- 3.5.5 Use of a City e-mail or IP address to engage in conduct that violates City policies or guidelines. Posting to a public newsgroup, bulletin board, or listserv with a City e-mail or IP address represents the City to the public; therefore, you must exercise good judgment to avoid misrepresenting or exceeding your authority in representing the opinion of the company.

4 Enforcement

An employee found to have violated this practice may be subject to disciplinary action, up to and including termination of employment. A violation of this practice by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with the City.

5 Definitions

Term	Definition
honeypot, honeynet	Network decoys that serve to distract attackers from valuable machines on a network. The decoys provide an early warning for intrusion detection and detailed information on

	vulnerabilities.
Spam	Electronic junk mail or junk newsgroup postings. Messages that are unsolicited, unwanted, and irrelevant.