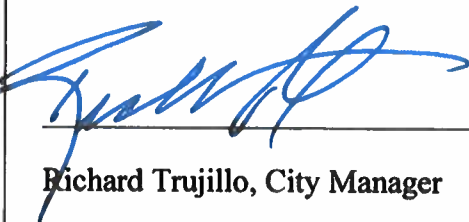


CITY OF LAS VEGAS
ADMINISTRATIVE REGULATIONS



SUBJECT: Acceptable Use of City IT Assets

ADMINISTRATIVE NUMBER: A17-232
REVISION: 1
SUPERSEDES:
EFFECTIVE DATE: 12/19/17
PAGES: 7

APPROVED BY:

Richard Trujillo, City Manager

OVERVIEW

The Information Technology Division's intentions for publishing an Acceptable Use of city IT Assets Policy are not to impose restrictions that are contrary to the city's established culture of openness, trust and integrity. The Information Technology Division is committed to protecting city employees, partners and the City of Las Vegas from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, mobile devices, and FTP, are the property of The City of Las Vegas. These systems

are to be used for business purposes in serving the interests of the city, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every city employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

1. PURPOSE

The purpose of this policy is to inform authorized users of city information technology assets of the appropriate and acceptable use of information, computer systems and devices. These rules are in place to protect the employee and the City of Las Vegas. Inappropriate use exposes the city to risks including virus attacks, compromise of network systems and services, and legal issues.

2. SCOPE

This policy applies to the use of information, electronic and computing devices, and network resources to conduct City business or interact with internal networks and business systems, whether owned or leased by city, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at City of Las Vegas and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with city policies, and federal and local laws and regulation.

Where conflicts exist between this policy or federal regulations, the more restrictive policy shall take precedence.

**ATTACHMENTS: ATTACHMENT A - Acceptable Use Agreement
ATTACHMENT B – IT Asset Incident Report**

3. POLICY

Guidelines:

The internet and other information technology resources are important assets that the city can use to gather information to improve external and internal communications and increase efficiency in business relationships. To encourage the effective and appropriate use of the city IT resources, the following policies govern the use of the city's IT resources:

- a. CLV shall provide all users with a written copy of this policy.
 - All users shall sign and date Attachment A- Acceptable Use Agreement
 - Each user's signed agreement shall be kept on file for as long as the user is employed by, has a contract with or otherwise provides services to the city.
- b. For the purpose of this policy, IT resources usage includes but not limited to all current and future internet/intranet communications services, the world wide web, voice over IP, file transfer protocol (FTP), TELNET, email, peer-to-peer exchanges, and various proprietary data transfer protocols and other services.
- c. The city may undertake all prudent and reasonable measures to secure the systems it uses for internet communications and the data transmitted by these systems and services, at the direction of the city CIO/IT manger or designee(s).
- d. The city may install software and/or hardware to monitor and record all IT resources usage, including email and web site visits. The city retains the right to record or inspect all files stored on city systems.
- e. City IT resources shall be used solely for city business purposes (except as described in this section of this policy) and users shall conduct themselves in a manner consistent with appropriate behavior standards as established in existing city policies. All city policies relating to intellectual property protection, privacy, misuse of city equipment, sexual harassment, sexually hostile work environment, data security, and confidentiality shall apply to the use of IT resources.
- f. Users shall have no expectations of privacy with respect to the city's IT resource usage. Serious disciplinary action up to and including termination of employment or contract may result from evidence of prohibited activity obtained through monitoring or inspection of electronic messages, files or storage devices. Illegal activity involving city IT resource usage may be referred to appropriate authorities for prosecution.

4. PROHIBITED INTERNET USE

City IT resources shall not be used for anything other than official city business unless otherwise specifically allowed by the official designee(s) or as permitted under this section of this policy.

- a. No software licensed to the city nor data owned or licensed by the city shall be uploaded or otherwise transferred out of the city's control without explicitly authorization from the city CIO/IT manager or appointed designee(s).
- b. IT resources shall not be used to reveal confidential or sensitive information, client/personnel data, or any other information covered by existing city, state, or federal

privacy or confidentiality laws, regulations, rules, policies, procedures, or contract terms. Users who engage in the unauthorized release of confidential information via the city's IT resources, including but not limited to newsgroups or chat rooms, will be subject to sanctions in existing policies and procedures associated with unauthorized release of such information.

- c. Users shall respect the copyrights, software, licensing rules, property rights, privacy, and prerogatives of others, as in any other business dealings.
- d. Users shall not use download executable software, including freeware and shareware, unless it is required to complete their job responsibilities.
- e. Users shall not use city IT resources to download or distribute pirated software or data, including music or video files.
- f. Users shall not use city IT resources to deliberately propagate any malicious code.
- g. Users shall not use city IT resources to intentionally disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of the city's network.
- h. Unauthorized access to communication rooms, server rooms, and rack cabinets is strictly prohibited.
- i. Unauthorized access to city network using personal devices is strictly prohibited.
- j. The city's IT resources shall not be used to establish connections to non-city internet service providers without prior authorization in writing by city CIO/IT manager and or appointed designee(s).
- k. Users shall not access, store, display, distribute, edit, or record sexually explicit or extremist material using the city IT resources.
- l. In departments/divisions where the display or use of sexually explicit or extremist materials falls within legitimate job responsibilities, a department/division head may exempt a user in writing from the requirements of this subsection. The department/division issuing the exemption letter shall keep the letter on file for as long as the user is employed by, has a contract with, or otherwise provides services to the city.
- m. The incidental and unsolicited receipt of sexually explicit or extremist material, such as might be received through email, shall not constitute a violation of this section, provided that the material is promptly deleted and neither stored nor forwarded to other parties.
- n. Users are prohibited from accessing or attempting to access IT resources for which they do not have explicit authorization by means of user accounts, valid passwords, file permissions or other legitimate access and authentication methods.
- o. Users shall not use city IT resources to override or circumvent any security mechanism belonging to the city or any other government agency, organization or company.
- p. Users shall not use city IT resources for illegal activity, gambling, or to intentionally violate the laws or regulations of the United States, any state or local jurisdiction, or any other nation.

5. PERSONAL USE OF THE INTERNET

Occasional and incidental personal use of the city's IT resources and internet access is allowed subject to limitations. Personal use of the internet is prohibited if:

- a. It materially interferes with the use of IT resources by the city or any political subdivision thereof; or
 - b. Such use burdens the city or any political subdivision thereof with additional costs; or
 - c. Such use interferes with the user's employment duties or other obligations to the city or any political subdivision thereof; or
- Such personal use includes any activity that is prohibited under this policy.

6. PASSWORD SECURITY

This policy establishes a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

- a. Passwords must be eight alphanumeric characters long; contain a number and symbol and cannot be a previous password.
- b. All system-level passwords (e.g., root, enables, NT admin, applications administration accounts, etc.) must be changed at least every 6 months. Password changes will be addressed immediately by the password authority when personnel changes are made to staff that have root access.
- c. Passwords must not be stored on unencrypted or other insecure forms (i.e., word document, post-its, labels, etc.).
- d. All user-level passwords (e.g., Tyler, Incode, email, web, desktop computer, domain, etc.) must be changed periodically; the minimum interval is every 3 months.
- e. User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- f. Passwords must not be inserted into email messages or other forms of electronic communication unless authorized by city CIO/IT Manger or appointed designee(s).
- g. All user-level and system-level passwords must conform to the guidelines set by the City of Las Vegas.
- h. Any web-based accounts used for city business, such as marketing or social networking shall assign administrative privileges to the CIO/IT Manager and/or the Public Information Officer. Any employee with access to such accounts shall be required to delete, remove, or reassign, their accounts when they separate from employment with the city.

7. PORTABLE DEVICES AND REMOVABLE MEDIA

- a. All portable computing resources and removable media shall be secured to prevent compromise of confidentiality or integrity. No computer device may store or transmit

sensitive information without suitable protective measures that are approved by city CIO/IT manger or appointed designee(s).

- b. When using computing devices such as notebooks, laptops, smartphones, and tablets, special care shall be taken to ensure that information is not leaked or compromised.
- c. Care shall be taken when using mobile computing devices in public places, meeting rooms, and other unprotected areas outside of the city's premises. It is important that when such devices are used in public places care shall be taken to avoid the risk of unauthorized persons viewing sensitive or protected information.
- d. Employees in the possession of portable, laptop, notebook, PDA, or other transportable computing device shall not check these computers in airline luggage systems or left in an unlocked vehicle. These computers shall remain in the possession of the traveler as hand luggage unless other arrangements are required by federal or state authorities.

8. SENSITIVE AND CONFIDENTIAL INFORMATION

- a. Sending documents containing sensitive and confidential information via fax, email, and/or through other media (e.g. flashdrive/thumbdrive, cloud share etc.) is prohibited unless required to perform job responsibilities.
- b. Using third-party email and/or other media services to send or receive sensitive and confidential information is prohibited unless approved in writing by city CIO/IT Manger or appointed designee(s).

9. REMOTE ACCESS

- a. Access to city networks from remote locations is not allowed except through the use of city-approved and city provided remote access systems and software. The city may allow remote access from non-city devices to access e-mail via a web browser. Only authorized users may be granted remote access. Must be approved in writing by city CIO/IT Manger or appointed designee(s).

10. REPORTING LOST OR STOLEN IT ASSETS

- a. In the event of theft or loss of city information, computer systems or portable devices, city users shall report the incident immediately to their direct supervisor and to the CIO/IT Manager or appointed designee(s).

ATTACHMENT A

Acceptable Use Agreement

I, _____ acknowledge I am being granted use of city information assets in order to carry out my work and agree that my use of such assets will be conducted in a manner that ensures compliance with this Policy and relevant law.

I understand my usage will be monitored, without further warning, and that inappropriate usage may be cause for disciplinary action, including but not limited to reprimand, suspension, and termination of employment or Civil or criminal prosecution under federal and state law.

I understand that I shall not use city portable devices when driving a motor vehicle. Any traffic violations or payment of fines imposed for violation of any applicable laws are my personal responsibility.

I understand that the use of city information assets may be revoked at any time without further warning.

I acknowledge, I have read and understood this document by signing below. I further understand it is my responsibility to seek advice regarding any questions I might have regarding this document or policy prior to my signing.

Employee Signature	Manager/Supervisor Signature	Date
Print Name	Print Name	Date