ITEM E

CITY OF LA VISTA
MAYOR AND CITY COUNCIL REPORT
MARCH 3, 2015 AGENDA

Subject:	Type:	Submitted By:
STANDARD OPERATION POLICY COMPUTER & E-MAIL USAGE POLICY	◆ RESOLUTION ORDINANCE RECEIVE/FILE	KEVIN POKORNY DIRECTOR OF ADMINISTRATIVE SERVICES

SYNOPSIS

A resolution has been prepared approving an update to the Standard Operation Policy regarding the Computer & E-Mail Usage Policy.

FISCAL IMPACT

N/A

RECOMMENDATION

Approval

BACKGROUND

A change to the Standard Operation Policy is proposed to update with changes in technology. 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 the City, the employee, or a third party. The policy was last updated in 2000. With changes in technology, it is imperative the computer and e-mail policies remain current with changes in technology to protect the city and its employees.

RESOLUTION NO. _____

A RESOLUTION OF THE MAYOR AND CITY COUNCIL OF THE CITY OF LA VISTA, NEBRASKA, APPROVING CHANGES AND REVISIONS TO AN EXISTING STANDARD OPERATION POLICY.

WHEREAS, the City Council has determined that it is necessary and desirable to create Standard Operation Policies as a means of establishing guidelines and direction to the members of the City Council and to the city administration in regard to various issues which regularly occur; and

WHEREAS, a Standard Operation Policy entitled Computer and E-Mail Usage has been reviewed and revisions recommended.

NOW, THEREFORE, BE IT RESOLVED, that the Mayor and City Council of La Vista, Nebraska, do hereby approve the changes to Standard Operation Policy entitled Computer and E-Mail Usage and do further hereby direct the distribution of said Standard Operation Policy to the appropriate City Departments.

PASSED AND APPROVED THIS 3RD DAY OF MARCH, 2015.

CITY OF LA VISTA

_____
Douglas Kindig, Mayor

ATTEST:

_____
Pamela A. Buethe, CMC
City Clerk

K:\APPS\City Hall\15 FINAL RESOLUTIONS\15. Amend SOP Computer And E-Mail Usage Policy 03.03.15.Docx

SUBJECT: COMPUTER & E-MAIL USAGE POLICY
DATE ISSUED: JUNE 2, 2000
ISSUED BY: CARA PAVLICEK, CITY ADMINISTRATOR
UPDATED: FEBRUARY __, 2015
ISSUED BY: BRENDA S. GUNN, CITY ADMINISTRATOR

1. Overview

The intent of this policy is to protect City of La Vista (City) employees, partners and the organization from illegal or damaging actions by individuals, either knowingly or unknowingly. This policy is not intended to impose restrictions that are contrary to the City's established culture of openness, trust and integrity.

Internet/Intranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and file transfer protocol, are the property of the City. 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.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at the City of La Vista. These rules are in place to protect the employee and the City. Inappropriate use exposes the City to risks including virus attacks, compromise of network systems and services, and legal issues.

3. 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 the City, the employee, or a third party. All employees are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with the City's policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2.

This policy applies to employees and to all equipment that is owned or leased by the City.

4. Policy

4.1 General Use and Ownership

4.1.1 City of La Vista proprietary information stored on electronic and computing devices whether owned or leased by the City, the employee or a third party, remains the sole property of the City.

The City's I.T. projects are managed by the I.T. Committee, which is comprised of representatives from all departments. The City's I.T. budget is set by the City Council and managed by the Director of Administrative Services.

4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of City of La Vista proprietary information.

4.1.3 You may access, use or share City of La Vista proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of

Internet/Intranet/Extranet systems. If there is any uncertainty, employees should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorized individuals within the City may monitor equipment, systems and network traffic at any time.

4.1.6 The City of La Vista reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

4.2.1 It is the responsibility of City employees, contractors, vendors and agents with remote access privileges to the City's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the City. All mobile and computing devices that connect to the internal network must comply with this policy.

General access to the Internet for recreational use by immediate household members on a City-issued device is prohibited.

4.2.2 Requirements

4.2.2.1 Secure remote access must be strictly controlled.

4.2.2.2 At no time should any City employee provide their log-in or e-mail password to anyone, not even family members.

4.2.2.3 City employees and contractors with network access privileges must ensure that their City-owned or personal computer or workstation, which is remotely connected to the City's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

4.2.2.4 Users are prohibited from utilized third-party e-mail systems and storage servers such as Google, Yahoo and MSN Hotmail to conduct City business such as creating binding transactions or to commit City resources. Such third-party systems may be used to monitor alerts for things such as news items and legislation.

4.2.2.5 Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

4.2.2.6 Non-standard hardware configurations must be approved by Sarpy County Information Systems and must approve security configurations for access to hardware.

4.2.2.7 All hosts that are connected to City internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers. Third party connections must comply with requirements as stated in the Third Party Agreement.

4.2.2.8 Organizations or individuals who wish to implement non-standard Remote Access solutions to the City production network must obtain prior approval from Sarpy County Information Systems.

4.2.3 Access via VPN

Approved City employees may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for providing their own Internet connection and wireless signal. Further details may be found in the Remote Access Policy.

Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to City internal networks.
2. All computers connected to City internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard; this includes personal computers.
3. VPN users will be automatically disconnected from the City's network after 30 minutes of inactivity. The user must then log-on again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
4. Only Sarpy County Information Systems-approved VPN clients may be used.

By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of the City's network, and as such are subject to the same rules and regulations that apply to City-owned equipment.

4.2.4 All City-owned computing devices must be locked or logged-off when they are unattended in a shared workspace environment. All users should lock their machine at the end of every day.

4.2.5 Postings by employees from a City e-mail address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the City, unless posting is in the course of business duties.

4.2.6 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of the City authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing City-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the City.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the City or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server or an account for any purpose other than conducting City business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using a City computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any City account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior notification to Information Systems is made.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network or account.
14. Introducing honeypots, honeynets, or similar technology on the City's network.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

4.3.2 E-mail and Communication Activities

When using City resources to access and use the Internet, users must realize they represent the City. Whenever employees state an affiliation to the City, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the City". Questions may be addressed to the Sarpy County Information Services Department

1. Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).
2. Any form of harassment via e-mail, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of e-mail header information.
4. Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited e-mail originating from within the City's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the City or connected via the City's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5. Policy Compliance

5.1 Compliance Measurement

The Sarpy County Information Systems team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the City.

5.2 Exceptions

Any exception to the policy must be approved by the Sarpy County Information Systems team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Definitions and Terms

Honeypot

Programs that simulate one or more network services that you designate on your computer's ports. An attacker assumes you're running vulnerable services that can be used to break into the machine. A honey pot can be used to log access attempts to those ports including the attacker's keystrokes. This could give you advanced warning of a more concerted attack.

Honeynet

A honeynet is a network set up with intentional vulnerabilities; its purpose is to invite attack, so that an attacker's activities and methods can be studied and that information used to increase network security.

Host

Any computer that has full two-way access to other computers on the Internet. Or a computer with a web server that serves the pages for one or more Web sites.

Spam

Electronic junk mail or junk newsgroup postings.

Split-tunneling

A computer networking concept which allows a VPN user to access a public network and a local network at the same time using the same physical network connection.

Dual-homing

A networked device is built with more than one network interface. Each interface or port is connected to the network, but one only one connection is active at a time. The other connection is activated only if the primary connection fails.