City of Grand Island

Tuesday, April 12, 2011
Council Session

Item I2

#2011-92 - Consideration of Amendment to the Personnel Rules Regarding Computer Usage

Staff Contact: Mary Lou Brown

Council Agenda Memo

From: Mary Lou Brown, City Administrator

Meeting: April 12, 2011

Subject: Replacing the City of Grand Island's Personnel Rules and Regulations, Section 3.06

Item #s: I-2

Presenter(s): Andrew Duey, IT Consultant

Background

Back in April of 2010, the Finance Department implemented electronic payments for utility bills and became "Payment Card Industry Data Security Standards" (PCI DSS) compliant. This involved transferring all customer credit card and bank account information previously housed on City servers to US Bank. In order to continue the City of Grand Island PCI DSS compliant status, a security awareness and acceptable use policy for all employees must be put into place. This policy must be reviewed by employees annually.

Discussion

The purpose of this policy is to outline the acceptable use of computer equipment at the City of Grand Island. The policy's goal is to protect the employees and the City of Grand Island. Inappropriate use can expose the City of Grand Island to risks including virus attacks, compromised network systems and services, and legal issues. The policy applies to all employees and equipment that is owned or leased by the City of Grand Island. The policy as presented replaces the current policy described in the City of Grand Island's Personnel Rules and Regulations, Section 3.06.

Alternatives

Alternatives to be addressed by the Council include the following:

1. Accept the recommended Security Awareness and Acceptable Use Policy in order for the City of Grand Island to remain PCI DSS compliant. The Policy is hereby incorporated into The City of Grand Island's Personnel Rules and Regulations, replacing Section 3.06.
2. Do not approve the Security Awareness and Acceptable Use Policy.

Recommendation

City Administration recommends that the Council approve the Security Awareness and Acceptable Use Policy and incorporate it into the City of Grand Island's Personnel Rules and Regulations, replacing Section 3.06.

Sample Motion

Move to approve the City of Grand Island Security Awareness and Acceptable Use Policy.

Sec. 3.06 CITY GOVERNMENT COMPUTER NETWORK

An e-mail system and Internet access are provided to City employees for the purpose of conducting official City business. These may not be used for prohibited purposes, such as conducting private business, or political campaigning, or any illegal uses. Personal use should be governed by the same tests of reasonableness as personal phone calls and internal e-mail. These include:

- There is no cost associated with the use
- Use is moderate in time
- Use does not interfere with an employee's or co-worker's work in either time or network bandwidth

Computers owned by City government or purchased with public funds should not have any recreational games installed. This includes the games supplied as part of the operating system of "free" additional programs. Contact the Information Technology Department and games will be removed that are already installed.

The Information Technology department will be notified whenever a new program is installed on a computer that is connected directly to the City Government Computer Network.

Because of the unique nature of the Internet, additional guidelines apply to its use:

- Internet access, hardware, and software must be authorized and installed by appropriate personnel in each City department. Employees authorized to download software or browser plug-ins should be provided with safety guidelines and virus protection software.

- Certain features of the Internet can clog the City's network and e-mail system and should be used only for work-related purposes. Examples would be:
    a. Listserv's, which generate large volumes of e-mail
    b. Streaming media, which uses large bandwidth
    c. Radio, music, and other downloading of a personal nature
    d. Continuous access services such as weather maps

- Resources, of any kind for which there is a fee, must not be accessed or downloaded without prior approval from the supervisor.
- Individual users must be aware of and at all times attempt to prevent potential City liability in their use of the Internet.

- Employees should be aware that there is a wide variety of information on the Internet. Some individuals may find some information on the Internet offensive or otherwise objectionable. Individual users should be aware that the City has no control over and can therefore not be responsible for the content of information available on the Internet.

Illegal uses or uses inconsistent with City policies including but not limited to gambling, sexually explicit materials, harassment, knowingly introducing of a computer virus or other harmful program, use of obscenities, violation of Copyright Laws, violation of any Local, State, and Federal Laws, etc. are prohibited.

City of Grand Island Security Awareness and Acceptable Use Policy

Overview

The intentions for publishing a security awareness and acceptable use policy are not to impose restrictions that are contrary to the established culture of openness, trust and integrity. The City of Grand Island is committed to protecting all employees, partners and the City of Grand Island 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, and FTP, are the property of the City of Grand Island. These systems are to be used for business purposes in serving the interests of the City of Grand Island, 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 of Grand Island 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.

Purpose

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

Scope

This policy applies to employees, contractors, consultants, temporary employees, and all other workers at the City of Grand Island, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the City of Grand Island.

Policy

General Use and Ownership

1. While network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the government systems remains the property of the City of Grand Island. Because of the need to protect the network, management cannot guarantee the confidentiality of employee's personal information stored on any network device belonging to the City of Grand Island.
2. An e-mail system and Internet access are provided to City employees for the purpose of conducting official City business. These may not be used for prohibited purposes, such as conducting private business, or political campaigning, or any illegal uses. Computer use on government systems may be audited.
3. Computers owned by City government or purchased with public funds should not have any recreational games installed. This includes the games supplied as part of the operating system of "free" additional programs. Contact the Information Technology Department and games will be removed that are already installed.
4. The Information Technology Department will be notified whenever a new program is installed on a computer that is connected directly to the City Government Computer Network.
5. For security and network maintenance purposes, authorized individuals within the City of Grand Island may monitor equipment, systems and network traffic at any time.
6. The City of Grand Island reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

City of Grand Island Security Awareness and Acceptable Use Policy

Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential. Examples of confidential information include but are not limited to: customer credit card information, employee information, customer receivable lists, vendor information and research data. Employees should take all necessary steps to prevent unauthorized access to confidential information.
2. Employees dealing with customer credit cards will not retain, email, or write down customer credit card information in any fashion.
3. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System and user level passwords will be required to be changed every 90 days.
4. All PCs, laptops and workstations will be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less. Employees should secure their workstations by logging off or locking (control-alt-delete for Windows users) when the host will be unattended. If for some reason a screen saver timeout interferes with system operation then special approval must be obtained from the IT department.
5. Postings by employees from a City of Grand Island email address to newsgroups, online forums, electronic bulletin boards or any other similar message posting systems should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the City of Grand Island.
6. All devices used by the employee that are connected to the City of Grand Island Internet/Intranet/Extranet, whether owned by the employee or the City of Grand Island, shall be continually executing approved virus-scanning software with a current virus database.
7. Employees must use extreme caution when opening e-mail attachments, which may contain viruses, e-mail bombs, or Trojan horse code.

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 device if that device is disrupting production services).

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

Certain features of the internet such as streaming media, radio or music stations can clog the City's network and e-mail system and should be used only for work-related purposes. Internet usage should not interfere with an employee's or co-worker's work in either time or network bandwidth.

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

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 of Grand Island.
2. 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.

3. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
4. 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.
5. Using a City of Grand Island 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.
6. Making fraudulent offers of products, items, or services originating from any City of Grand Island account.
7. 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.
8. Port scanning or security scanning is expressly prohibited unless prior notification to IT is made.
9. Executing any form of network monitoring which will intercept data not intended for the employee's device, unless this activity is a part of the employee's normal job/duty.
10. Circumventing user authentication or security of any device, network or account.
11. Providing information about, or lists of, City of Grand Island employees to parties outside the City of Grand Island.

Email and Communications Activities

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

Enforcement

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

Definitions

Spam Unauthorized and/or unsolicited electronic mass mailings.

R E S O L U T I O N 2011-92

WHEREAS, the City of Grand Island needs to continue compliance with the "Payment Card Industry Data Security Standards" (PCI DSS) requirement; and

WHEREAS, the City of Grand Island wants to adopt this Security Awareness and Acceptable Use Policy for all City of Grand Island employees; and

WHEREAS, Security Awareness and Acceptable Use Policy will be reviewed by all employees annually; and

WHEREAS, the City of Grand Island Security Awareness and Acceptable Use Policy has been reviewed and approved by the City Attorney's office;

NOW, THEREFORE, BE IT RESOLVED BY THE MAYOR AND COUNCIL OF THE CITY OF GRAND ISLAND, NEBRASKA, the City of Grand Island Security Awareness and Acceptable Use Policy is hereby approved and incorporated into the City of Grand Island's Personnel Rules and Regulations, replacing Section 3.06.

BE IT FURTHER RESOLVED, that the Mayor is hereby authorized and directed to execute such agreements on behalf of the City Of Grand Island.

- - -

Adopted by the City Council of the City of Grand Island, Nebraska, April 12, 2011.

_____

Jay Vavricek, Mayor

Attest:

_____

RaNae Edwards, City Clerk

Approved as to Form ¤ _____
April 8, 2011 ¤ City Attorney