Administrative Policy 16-2 Computer and Network Security Policy

DISTRIBUTION: All Departments

SUBJECT: City of Muskogee Computer and Network Security Policy

PURPOSE: The purpose is to outline the acceptable use of computer equipment at the City.

BACKGROUND:

POLICY/PROCEDURES: See attached EXHIBIT "A"

REFERENCES: None.

RESPONSIBLE DEPARTMENT: Information Technology

EFFECTIVE: This policy is in effect from the date of issuance until amended or rescinded.

Dated this 2 day of September, 2009.

Greg Buckley
City Manager

Approved as to form and legality this 31st day of Aug, 2009.

John H. Vincent, City Attorney

l:\cityattorney\council policies\administrative policies\working\16-2 computer and network security policy.docx

Exhibit "A"

City of Muskogee
Computer and Network Security Policy

1. Overview
   1.1. The intention of the IT department for publishing a Computer and Network Security Policy are not to impose restrictions that are contrary to the City's established culture of openness, trust and integrity. The IT Department is committed to protecting City employees, partners and the City from illegal or damaging actions by individuals, either knowingly or unknowingly.
   1.2. 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 Muskogee. These systems are to be used for business purposes in serving the interests of the City, and of our citizens in the course of normal operations.
   1.3. 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.
   1.4. Under this policy, the City of Muskogee may be referred to simply as "City" or "the City".
   1.5. A summary of this policy known as the "Acceptable Use Policy" shall be made available. The Acceptable Use Policy is not to be considered a replacement for this policy.
2. Purpose
   2.1. The purpose of this policy is to outline the acceptable use of computer equipment at the City. 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
   3.1. This policy applies to employees, contractors, consultants, temporaries, and other workers at the City, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the City.
   3.2. This policy applies to any vendor or support staff not directly employed by the City of Muskogee, but accessing resources owned and/or managed by the City.
4. General Use and Ownership
   4.1. While the City's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the City's systems remains the property of the City. Because of the need to protect the City's network, management cannot guarantee the confidentiality of information stored on any network device belonging to the City.
   4.2. 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. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
   4.3. For security and network maintenance purposes, authorized individuals within the City may monitor equipment, systems and network traffic at any time.
   4.4. The City reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
5. Security and Proprietary Information
   5.1. General Security
      5.1.1. All PCs, laptops and workstations will be secured by locking the computer or by logging-off when the host will be unattended. The computer will automatically lock after 15 minutes of inactivity.
      5.1.2. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "Laptop Security Tips".
   5.2. Password Policy
      5.2.1. Except for generic accounts, passwords uniquely identify the user. The user is responsible for any and all activity under his or her password. Any violations to this or any policy occurring with the use of an account will be identified with the owner of that account.
      5.2.2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.

5.2.3. Passwords are to be kept private and not shared with anyone under any circumstances. Passwords revealed to IT staff for troubleshooting purposes should be changed immediately by the user once the problem has been resolved.
5.2.4. User level passwords should be changed every 42 days.
5.2.5. Passwords must contain at least seven characters, at least 1 number, 1 letter, and 1 capital letter.
5.2.6. Passwords should not be found in any dictionary, English or foreign.
5.2.7. Passwords should not be a common usage word such as:
5.2.7.1. Names of family, pets, friends, co-workers, fantasy characters, etc.
5.2.7.2. Computer terms and names, commands, sites, companies, hardware, software.
5.2.7.3. Birthdays and other personal information such as addresses and phone numbers.
5.2.7.4. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
5.2.7.5. Any of the above spelled backwards.
5.2.7.6. Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
5.2.8. Passwords should have the following characteristics:
5.2.8.1. Contain both upper and lower case characters (e.g., a-z, A-Z)
5.2.8.2. Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
5.2.8.3. Are at least seven alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).
5.2.8.4. Are not a word in any language, slang, dialect, jargon, etc.
5.2.8.5. Are not based on personal information, names of family, etc.
5.2.8.6. Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

5.3. Network Security
5.3.1. No device shall be connected to the City's network without the approval of the IT department.
5.3.2. No device which is not owned by the City and/or managed by City IT Staff shall be connected to the City's network.
5.3.3. All hosts used by the employee that are connected to the City network shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.

5.4. Wireless Security
5.4.1. No wireless access point or network shall be installed on the City network without the express permission of the IT Director.
5.4.2. Wireless Ad-hoc (peer-to-peer) networks shall not be used with City owned computers.

5.5. Email and Web Security
5.5.1. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
5.5.2. Downloading of executable software, installers, scripts, macros, etc. without IT department approval is strictly forbidden.
5.5.3. Downloading any copyrighted data, music (WAV, MP3, etc), video, or other copyrighted content to which the City does not have rights to is strictly forbidden. This includes copying music from personal music CDs to the computer.

5.6. Account Policies
5.6.1. As a general policy, no user shall have an administrative account or elevated rights.
5.6.2. Accounts associated with an email (exchange) account shall not have rights as a Domain Administrator.
5.6.3. Administrative accounts will be limited to IT Staff users. Departmental "Super Users" may be designated by the IT Director and by whose discretion be assigned elevated rights to the domain or local computer.
5.6.4. Individual user rights may be temporarily elevated at IT staff discretion for the purpose of troubleshooting, allowing the user to install approved software or demos, or to provide temporary resolution to a problem until a permanent solution can be found and implemented.

6. Personal Use
6.1. In general, personal use of City computers and resources is allowed under this policy providing that such use does not impact the employee's performance of his or her duties and does not violate this policy,

individual department policy, or any other policy of the City of Muskogee including, but not limited to, the Unacceptable Use section of this policy.

6.2. Any personal data stored on or transmitted by or through City owned resources are the property of the City of Muskogee and subject to review or monitoring at any time.

7. 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.

7.1. System and Network Activities

7.1.1. The following activities are strictly prohibited, with no exceptions:

7.1.1.1. 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 City.

7.1.1.2. 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 City or the end user does not have an active license is strictly prohibited.

7.1.1.3. 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.

7.1.1.4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

7.1.1.5. 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.

7.1.1.6. 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.

7.1.1.7. 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, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

7.1.1.8. Port scanning or security scanning is expressly prohibited unless prior notification to the IT Department is made.

7.1.1.9. Circumventing user authentication or security of any host, network or account.

7.1.2. Email and Communications Activities

7.1.2.1. 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).

7.1.2.2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

7.1.2.3. Unauthorized use, or forging, of email header information.

7.1.2.4. 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.

7.1.2.5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

7.1.2.6. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

7.1.2.7. Virus or Malware warnings are not to be transmitted to other employees by anyone except IT staff. This is due to the vast number of hoaxes being propagated throughout the internet.

8. Network Policy
    8.1. Allowed Devices
        8.1.1. Only devices owned by the City of Muskogee and managed by the IT Department shall be allowed to access, wired or wirelessly, to the City of Muskogee's internal network or subnets.
        8.1.2. Connected devices shall conform to the antivirus and security standards currently in use by the IT department.
    8.2. Prohibited Devices
        8.2.1. Personally-owned devices shall not be connected to the City's network or to any computer, printer, server, etc.
        8.2.2. Wireless access points other than those installed and managed by the IT department shall be prohibited.
    8.3. Wireless Devices
        8.3.1. Wireless peer-to-peer (ad-hoc) connections should not be used at any time.
    8.4. VPN (Virtual Private Network) Policy
        8.4.1. Devices
            8.4.1.1. With the exception of approved vendors, only City-owned computers may access the City network via VPN.
        8.4.2. Employees
            8.4.2.1. Only employees with an urgent need may connect to the City network via VPN and then only from a City-owned computer.
        8.4.3. Vendors
            8.4.3.1. Vendors may have specific access to systems they support through VPN. This may be an always-on connection, or an on-demand client connection.
9. Policy Revisions and exceptions
    9.1. This policy may be revised or amended from time to time as technology changes or new threats are discovered.
    9.2. An exception to this policy may be made on an individual basis in order to respond to a departmental need. Any exceptions to this policy must be approved by the IT director or an authorized delegate.
    9.3. An IT Committee consisting of one delegate from each department may be formed to help create and revise IT Policy. The purpose of this committee shall be to communicate departmental needs to the IT department and to allow the IT department to communicate issues back to each department.
    9.4. Revision History
        9.4.1. 7/31/07 – Policy created.