Document Type: Policy
Category: Administration
Domain: Service Delivery
Owner: IT Administration

Information Technology

Information Systems Acceptable Use Policy

City of Oklahoma City

Issue Date: 9/2015
Effective Date: 9 /2015
Review Date: Annual

Purpose

The purpose of this policy is to define acceptable use of The City of Oklahoma City's (the City) information technology resources and expected end-user behavior in order to protect critical information and safeguard information technology resources.

Scope

This policy applies to all users of computers, network, communications systems and data controlled, owned, operated or supported by the City of Oklahoma City.

Philosophy

The information technology resources provided to users are for the benefit of enhanced and improved productivity in service to our customers and to the Citizens of this City. It is each user's responsibility to apply the following philosophies in the use of these resources:

1. All users will comply with local, state, and federal laws or regulations regarding the use of the City's information technology resources.

2. Users shall refrain from inappropriate use of the City's resources including, but not limited to the following:

    a. Conducting an outside business

    b. Supporting, promoting, or soliciting for an outside organization or group unless otherwise provided by permit or agreement with the City. (e.g., City co-sponsored events)

    c. Political campaigning

    d. Commercial purposes such as advertising or selling unless otherwise provided by permit, or agreement with the City (e.g., Civic Center events)

    e. Illegal activities

    f. Activities that would cause embarrassment to the City including, but not limited to sexually explicit or otherwise inappropriate acts

    g. Harassment of other employees

3. The City will not bear the financial burden of any personal or private activities that involve use of information technology resources.

4. All users will be subject to monitoring of their use of information technology resources.

Policy Statement

Section I. Data Management

1. All technology equipment purchased by the City of Oklahoma City and all data, including email, either created or received, that is placed on City owned or maintained equipment, network, storage devices or other systems is the property of the City. All equipment and data owned by the City is subject to being intercepted, monitored, read, searched or seized without prior notice at any time.

2. Users are prohibited from installing, downloading or executing any software that has not been approved by the Information Technology (IT) Department.

3. All shares will be authorized by the department-designated contacts and will be secured.

4. Users are responsible for securing and recovering data they store in any location other than on the City Network or in "My Documents" this would include the local hard drive.

5. Permanent storage of City business related data and documents must reside only on the City's network storage system. Temporary use of removable media for purpose of meetings and file transfer may be permitted; however, copies stored on removable media (external drives, USB drives, DVDs, CDs, etc.) must meet Purchase Card Industry Data Security Standards (PCI DSS) and Personal Identifying Information (PII) requirements (e.g., encryption). Regardless, the principal copy of the City data and documents should not be kept on removable media without the approval of the IT Director.

Section II. Email

1. City email accounts should be used primarily for business purposes. Personal communication is permitted on a limited and minimal basis. Non-City related commercial uses are prohibited.

2. Registration or other use of City email addresses for non-business related internet services or other web communications is prohibited. Any registrations for business use must not use the combination of City email address and user's City password.

3. All use of email must be consistent with City policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices. The City email system shall not to be used for the creation or distribution of any messages which are discriminatory, abusive, disorderly, disruptive, or retaliatory. Employees who receive any emails with this content from any other employee or outside party (not including spam type emails) should report the matter immediately to their supervisor. (Refer to Article 400 of the *City of Oklahoma City Personnel Policies* and PSB containing the *Policy Prohibiting Discrimination and Sexual Harassment*.).

4. Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct City business or to store or retain City email. Further, users are prohibited from automatically forwarding City email to any third party email system or alternative off-network (non-discoverable) storage.

5. Spam email entering the City email system are filtered through an automated email filtering system to remove emails which may have inappropriate content, contain viruses or malware, or otherwise pose a security risk. Not all emails which would be regarded as spam will be filtered with this automate process. It is up to the employee to report to the IT Service Desk any email which they believe poses a security risk or is offensive to the point that filters should be updated to attempt to block this type of content.

6. Employees are expected to be vigilant in guarding against phishing or other fraudulent emails. For suspected phishing or other fraudulent emails, employees should not open, reply, or click on embedded links. While these emails will almost always come from outside the City network, they could also come from internal users if their account has been compromised. Users must immediately report to the IT Service Desk specific emails which may pose a security threat to the City or any incidents where they believe their account or City system may have been compromised.

7. Users are responsible for the disclosure and handling of confidential or Personal Identifying Information (PII) contained in email messages (Refer to Section 410 – "Access to Confidential Information" of *The City of Oklahoma City Personnel Policies*). Limit the internal forwarding of emails which contain confidential or Personal Identifying Information (PII). Emails which are sent outside the City network for business purposes which contain confidential or Personal Identifying Information (PII) must be encrypted using the *Email Encryption Summary and Basic Instructions.*

8. Users shall not send mass emails containing personal messages to more than 10 recipients. Mass emails for City business purposes are permissible.

9. Users shall not misrepresent or forge the identity of the sender or source of an electronic communication.

10. It is the user's responsibility to stay within mailbox size limitations.

11. Users shall use the default email template and refrain from the following:

    a. Changing colors, style, font or stationery of the email to a format inappropriate for business communications
    b. Inserting non-business related pictures, movies or animation
    c. Using any background other than the default white background
    d. Adding non-business messages, quotations or emoticons (a symbol or combination of symbols used to convey emotional content such as a smiley face) in business related messages

12. Employees shall have no expectation of privacy in anything they store, send or receive on the City's email system.

13. Emails are retained indefinitely on-line until deleted by the user. Once a user deletes an email message, calendar item, contact, task or note the items will be automatically retained and discoverable for a period of 60 days. Upon request of City Manager, Assistant City Manager, City Auditor, Municipal Counselor, Personnel Director, Department Head or designee, a "litigation hold" may be placed on an email account which will result in all items being retained while the hold is in place for the purpose of recovery, litigation, or Personnel investigation; employees may not be notified of this "litigation hold".

14. Email searches are only executed as directed by the City Manager, Assistant City Manager, City Auditor, Municipal Counselor, Personnel Director, Department Head or designee, and in fulfillment of an open records request through the City Clerk's office.

Section III. Access to Employee's Email and Files

1. Access to existing or former employee emails or electronically stored files requires Department Head approval.

2. The City may be required to produce and disclose relevant information and records in compliance with applicable law, court order, and/or agreement made during the litigation process. Therefore, an employee's

computer or other electronic device may be searched in order to comply with any applicable law, court order or agreement.

Section IV. Security Breach

1. All Personal Identifying Information (PII), as defined herein, that is sent outside of the organization, via email or other electronic means must be redacted or encrypted. Departmental Supervisors and IT personnel are available to recommend means to protect PII while still conducting the City's business.

2. All information must be reviewed on a case-by-case basis for PII before being disclosed, transmitted or otherwise provided to others outside the City's organization.

3. Users are responsible for protecting sensitive City data from unauthorized access, including but not limited to, data available outside of the City network, on mobile computers, removable media, mobile devices or email.

4. State law mandates the reporting of lost or unauthorized acquisition of any PII that is unencrypted or un-redacted. Therefore, users must report the loss, suspected loss, or missing sensitive data immediately to their supervisor and the IT Service Desk.

Section V. Incident Handling

1. All incidents and service requests must be reported to the Service Desk.

2. "Critical" incidents must be reported by telephone or in person.

    a. If 297-2727 is not available, escalate through your chain of command to Information Technology Management as listed in the Emergency Contacts List.

Section VI. Internet/Intranet

1. No user will be granted access to the Internet without proper approval by their department management.

2. Users shall not access sites that may violate federal, state or local laws or could cause embarrassment to the City.

3. Users shall not access personal web mail such as Cox, Hotmail, Yahoo, etc. using City resources.

4. Internet usage that impacts productivity will be determined and monitored by department management. IT reserves the right to suspend

Internet Services of any user that is negatively impacting the City's network resources.

5. City technology resources such as web pages and data sharing locations that are for communication among City employees shall be used only to promote City purposes or programs approved by the Mayor, City Council, and/or City Manager.

6. City technology resources such as web pages and data sharing locations that are intended as official communication from the City to the general public shall only be used to promote City purposes or programs approved by the Mayor, City Council, and/or City Manager. No employee personal messages are permitted on these locations.

Section VII. Instant Messaging

Instant messaging clients such as Yahoo, AOL, and MSN Instant Messaging that communicate outside the City's network are not allowed.

Section VIII. Modems

1. No user will install a modem on any City-owned equipment without prior authorization from IT.

2. No user can modify any existing modems, including location or configuration, without prior authorization from IT.

Section IX. Network

No user shall add or change any component on the City's network without proper approval by IT.

Section X. Client Systems

1. Employees utilizing mobile computing devices such as laptops or Personal Data Assistants (PDA's) are responsible for protecting information from unauthorized access and protecting the City's equipment from theft or vandalism.

2. No changes to the security configuration of client devices or systems, such as, changing bios passwords or adding local administrator accounts, without authorization from IT.

3. Users must report the loss of technology hardware to their department management, the IT Service Desk and if appropriate, the applicable Law Enforcement Agency.

4. Users will contact the IT Service Desk before purchasing or installing any new computing devices.

5. No personal devices will be allowed to connect to the City's network except as provided under the Remote Access policy.

Section XI. Remote Access

1. Remote access must be authorized by the appropriate level of approval within the Department and a completed Remote Access form must be on file in IT.

2. Users will ensure the remote computer meets the following requirements:

    a. Up-to-date anti-virus software and latest virus definitions

    b. Latest Operating System service pack and critical updates

    c. Physically secure computer

3. Password authentication will be required to enhance security and reduce the risk of unauthorized access to the network.

Section XII. Sign-on/Passwords

1. Using or attempting to use the computer accounts of others is prohibited.

2. Passwords are Personal and Private Information and shall be kept confidential and never shared.

3. User's domain passwords must comply with the following:

    a. Passwords must be a minimum of 8 characters in length; contain at least one number and one special character (if the system permits special characters).

    b. Numeric and special characters can be placed at the beginning or end as long as at least one numeric or special character is imbedded somewhere else within the password.

    c. The password must not contain the user name or the person's name.

    d. Clear text passwords must not be imbedded in connectivity scripts or programmed into PF keys.

4. Two factor authentication (Token) users may use a four digit PIN number that never expires.

Section XIII. Telephone

1. No user will move telecommunications or voicemail equipment without prior authorization from IT.

2. Use of business or cellular phones for purposes other than Official City Business is permitted only under limited circumstances, such as:

    a. There is no cost to the City or the accumulated cost to the City is de minimis

    b. It does not interfere with the employee's official duties

    c. It is brief in duration, including an accumulation of time used

    d. It does not compromise the security or integrity of City information

3. All cellular services used must be specifically authorized by the Department Head in advance.

    a. Examples of costs not covered under normal plans are information use (411), text messaging, ringtones, and long distance.

4. Costs resulting from personal use of phones must be reimbursed to the City Treasurer within 30 days of billing.

5. In cases where the Department is notified of telephone use that resulted in additional costs to the City:

    a. The Department is responsible for determining if the cost was due to personal use.

    b. The Department must document the outcome of the additional cost determination, noting if the costs were business related or personal.

    c. If the use is personal and resulted in costs to the City, the Department is responsible for ensuring appropriate payment is made to the Treasurer's Office.

    d. Documentation should be retained per the City's Record Retention Policy.

Section XIV. Video and/or Audio Streaming

Video and/or audio streaming affects the City’s overall internet performance and should only be used for Official City Business.

Definitions

Personal Identifying Information (PII) – sensitive data, including but not limited to the last name, first name or initial in combination with and is linked to a personal identifier such as Government Issue number, date of birth, financial number, or similar data that could link an account to a specific person. PII does not include information lawfully obtained from publicly available sources as allowed by law.

Sensitive data - any information that could adversely affect the interest or privacy of individuals when lost, modified or acquired through unauthorized access. Sensitive data generally includes un-redacted or unencrypted personal identification information (PII) and may include any of the following:

Dates of Birth
Social Security Numbers
State ID or Driver License Numbers
Military ID numbers
Home or Cell Telephone numbers
Credit card information or CVS (Card Verification System)
Medical Information
Account information relating to account numbers or other information that can link an account to a specific person.
Any Juvenile Information

In addition, the home address of any existing or former employee is considered confidential pursuant to the Open Records Act, 11 O.S. § 24A.1, et Seq..

Redacted - for the purpose of this policy means alternating or truncating data so that no more than 5 digits of any social security number or 4 digits of a driver license, an ID number, or financial account information is accessible.

Encrypted - for the purpose of this policy means scrambling of electronic data using an algorithmic mathematical formula to prevent unauthorized disclosure of the data

Security Breach - for the purpose of this policy means the unauthorized access and/or acquisition of unencrypted and un-redacted data containing personal identifying information.

Responsibilities

Steering Committee

- Responsible for the review and approval of the Acceptable Use Policy (AUP).

IT Security

- Responsible for coordinating with the Municipal Counselors' Office to determine if and/or how any notification should be done to comply with the law.

Technology Advisory Committee

- Responsible for providing departmental input regarding the policy.

Department Heads, Managers, Supervisors

- Responsible for requiring all staff under their management read and acknowledge this policy and abide by the provisions of this policy.

IT Director

- Responsible for reviewing the policy and making any necessary changes.

- Responsible for reviewing and documenting requests for exceptions to the AUP.

User Community

- Responsible for becoming familiar with the policy, understanding the expectations and taking personal responsibility for adhering to the provisions of this policy.

- Acknowledge their understanding of the policy and agreement with the provisions by signing electronically after completing the online training.

Contractors, Vendors, or Volunteers

- Responsible for adhering to this policy and acknowledging an awareness of the policy.

Exceptions

Any exceptions to the AUP must be in writing and submitted to the IT Director for approval. All approved exceptions will be reviewed by the Steering Committee.

Exceptions will be documented and filed in the IT department. It will be the responsibility of the IT Director to respond in writing to the exception requests once a decision has been made. All exceptions will be reviewed on an annual

basis. Exceptions will be documented following the Policy Exception Documentation Procedures.

Disciplinary Actions

IT management will review alleged violations of the Acceptable Use Policy on a case-by-case basis. Clear violations of this policy will be reported to the appropriate department/division head and may result in suspension or termination of services

Violations of the policy may result in discipline, up to and including termination.