DEPARTMENT OF INFORMATION TECHNOLOGY

CITY HALL • 340 NORTH WASHINGTON AVENUE • SCRANTON, PENNSYLVANIA 18503 • PHONE: 570-969-6658 • FAX: 570-348-4148

CITY OF SCRANTON ACCEPTABLE USE STANDARDS FOR INFORMATION TECHNOLOGY RESOURCES

Each Authorized User of City of Scranton Information Technology resources must comply with these standards when using Scranton IT resources.

AUDITING AND REPORTING

Scranton reserves the right to monitor and/or log, with or without notice, all Internet activity, all Internet web site access, all E-Mail and any other communications or data accessed, stored or otherwise used by or on Scranton IT resources. Therefore, Authorized Users should have no expectation of privacy in the use of Scranton IT resources. Authorized Users are encouraged to assist in the enforcement of these standards by promptly reporting any observed violations to their supervisor or the Human Resources Office. All physical equipment, intellectual property, information, software, data, files or programs that are provided, stored or otherwise utilized by or on any Scranton IT resource is the property of The City of Scranton.

DISCIPLINE

Misuse of Scranton IT resources by employees or volunteers may result in disciplinary action, up to and including termination, depending on the circumstances of the incident. The improper use of Scranton IT resources by contractors or consultants may result in disciplinary action that may include formal action. When warranted, Scranton may pursue or refer matters to other authorities for criminal prosecution against persons who violate local, state, or federal laws through the use of Scranton IT resources.

GENERAL IT RESOURCE USE

a. As part of the privilege of being an Authorized User, Authorized Users may not attempt to access any data or programs contained on Scranton systems for which they do not have authorization and/or explicit consent.
b. Authorized Users may not share their City of Scranton account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes with any other person or Authorized User. Authorized Users are strictly responsible for maintaining the confidentiality of their City or Scranton account(s), passwords, PIN, Security Tokens or similar information or device.
c. Authorized Users may not make unauthorized copies of copyrighted software.
d. Authorized Users may not use non-standard shareware or freeware software.
e. Authorized Users may not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of IT Resources; deprive an Authorized User of access to an IT resource; obtain extra IT Resources beyond those allocated; or circumvent computer security measures.
f. Authorized Users may not use Scranton IT resources for personal gain.
g. Authorized Users may not engage in illegal activity in connection with their use of Scranton IT Resources, including, but not limited to downloading, installing or running security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, Authorized Users may not run password cracking programs, packet sniffers, port scanners or any other non-approved programs on Scranton IT resources unless they are specifically authorized to do so.
h. Authorized Users may not intentionally access, create, store or transmit material that is generally considered to be inappropriate or personally offensive, including sexually suggestive, pornographic or obscene material.
i. Authorized Users may not utilize unauthorized proprietary and/or commercial Instant Messaging (IM) products on Scranton computer resources.
j. Authorized Users are personally responsible for the security of authorized portable Scranton IT resources such as issued laptops, Blackberries and cell phones. Care must be exercised to ensure these devices are not lost, stolen or otherwise accessed in an unauthorized manner. If an IT resource is lost users must inform the Department of Information Technology immediately.
k. Authorized Users may not store non-public information on IT resources, if those IT resources will be removed from Scranton's facilities without prior approval from their supervisor.
l. Authorized Users may only use encryption methods approved by Scranton to encrypt information.
m. Authorized Users may not use non-Scranton or non-approved storage devices or storage facilities.

INTERNET USE

All security policies of the City and its departments, as well as policies of Internet sites being accessed, must be strictly adhered to by Authorized Users.

Software

In connection with Authorized Users' use of and access to Scranton IT Resourses:

a. All software used to access the Internet must be part of Scranton's standard software suite. This software must incorporate all vendor provided security patches.

b. All files downloaded from the Internet must be scanned for viruses using the approved City of Scranton distributed software suite and current virus detection software.

c. All software used to access the Internet shall be configured to use an instance of Scranton's standard Internet Access Control & Content Filtering solution.

Expectation of Privacy

a. Authorized Users may not rely on any communications via the Internet using Scranton IT resources being secure, private, or inaccessible, except where appropriate security applications are used, e.g. data encryption.

b. All activity on Scranton IT resources is subject to logging and review.

Access Control and Authorization

Departments should authorize access to the Internet using Scranton computer resources through the utilization of a user ID/password system. Security violations can occur through unauthorized access and all possible precautions should be taken to protect passwords. Authorized Users are responsible for activity and communications transmitted under their account.

Incidental Use

a. Use of Scranton IT resources is only authorized for personal use on a limited, occasional, and incidental basis and in a manner consistent with this policy.

b. Incidental personal use of Internet access is restricted to Authorized Users; it does not extend to family members or other acquaintances.

c. Access to the Internet from a Scranton owned, home based computer must adhere to all the same policies that apply to use from within The City of Scranton's facilities. Employees may not allow family members or other non-employees to access Scranton computer systems.

d. Incidental use must not result in direct costs to Scranton.

e. Incidental use must not interfere with the normal performance of an Authorized User's work duties.

f. No user may send or solicit files, documents or data that may risk legal liability for, or embarrassment to, Scranton.

g. All files and documents located on Scranton IT resources, including personal files and documents, are owned by Scranton and may be accessed in accordance with this policy.

Acceptable Use of the Internet

Accepted and encouraged use of the Internet for Authorized Users on Scranton IT Resources includes, but is not limited to, the following:

1. Access, research, exchange, or posting of information that relates to the assigned job duties of an Authorized User for carrying out Scranton's business.

2. Promotion of public awareness in regard to Scranton's laws, Scranton's services, and public policies.

3. Posting of city information that has been authorized by appropriate management.

E-MAIL USE

Expectation of Privacy

a. When sensitive material is sent electronically via E-mail, it is important to verify that all recipients are authorized to receive such information and to understand that E-mail is not fully secure and/or private, except where appropriate security applications are used, e.g. data encryption.

b. Users should understand that messages can be quickly and easily copied and may be forwarded inappropriately.

c. Where it is necessary to transmit Scranton's proprietary or restricted information beyond Scranton's E-mail network, the messages should be protected by encryption. Authorized Users should contact the Department of Information Technology for assistance if encryption is needed.

d. E-mail messages to be transmitted outside of the United States should comply with local laws governing international transmission of data as well as United States export control regulations. For assistance, Authorized Users should contact the Department of Information Technology.

e. Department Managers should determine specific policy regarding business information which is determined to be too confidential or sensitive to be transmitted via E-mail.

f. All user activity on Scranton IT resources is subject to logging and review.

Access Control and Authorization

a. Only Authorized Users may use Scranton IT resources to send or view E-mail or access Scranton's E-mail systems.

b. Unauthorized persons may not use the network or Scranton equipment to originate E-mail messages or read E-mail messages directed to others.

c. Access to Scranton's E-mail will only be granted to Scranton workforce members, including employees, contractors, consultants, volunteers and other authorized users if they agree to abide by all applicable rules of the system, including this policy and its related standards.
d. Unauthorized access of an Authorized User's E-mail files is a breach of security and ethics and is prohibited. An Authorized User may not access the E-mail or account of another Authorized User unless granted permission to do so by the Authorized User. This restriction does not apply to system administrators and management staff who are authorized to access E-mail for legitimate business purposes.
e. In accordance with Scranton's policy, Authorized Users should use password protection to limit access to E-mail files. Authorized Users must safeguard their passwords so that unauthorized users do not have access to their E-mail. Authorized Users are responsible for messages transmitted under their account.

Message Retention

E-mail messages may be subject to Scranton's document retention standards.

E-mail Security Issues – Worms & Viruses

E-mail and attachments to E-mail increasingly are reported to be sources of computer viruses. All Authorized Users should perform a virus scan on attachments before opening them.

Maintaining Professionalism.

Every Authorized User who uses Scranton computer resources is responsible for ensuring posted messages are professional and businesslike. As a way to impose personal restraint and professionalism, all employees should assume that whatever they write may at some time be made public.

Authorized Users should follow the following guidelines:
1. Be courteous and remember that you are representing The City of Scranton with each E-mail message sent.
2. Review each E-mail message before it is sent and make certain that addresses are correct and appropriate.
3. Consider that each E-mail message sent, received, deleted, or stored has the potential to be retrieved, seen, and reviewed by audiences, including the general public, who were not the intended recipient of the message.
4. Ensure that content is appropriate and consistent with business communication; avoid sarcasm, exaggeration, and speculation which could be misconstrued.
5. Be as clear and concise as possible; be sure to clearly fill in the subject field so that recipients of Email can easily identify different E-mail messages. Avoid subject fields that are vague and general, e.g. "question," "comment," etc.

Electronic Message Distribution, Size and Technical Standards

a. Authorized Users should receive authorization from their supervisor or their superior before wide scale "broadcasting" of an E-mail bulletin to groups of employees.
b. The use of "reply to all" should be avoided unless it is appropriate to respond to all addressees.
c. Authorized Users wishing to send E-mail bulletins to all City of Scranton employees must first obtain authorization from management or their supervisor.
d. E-mail messages should be brief and attachments to E-mail messages should not be overly large.

UNACCEPTABLE USES OF IT RESOURCES

The following are examples of impermissible uses of Scranton IT resources. This list is by way of example and is not intended to be exhaustive or exclusive. Authorized Users are prohibited from:
1. Viewing, accessing, posting or transmitting any material that is generally considered to be personally offensive or inappropriate, including sexually suggestive, pornographic, or obscene materials.
2. Viewing, accessing, posting or transmitting material that expresses or promotes discriminatory attitudes toward race, gender, age, nationality, religion, or other groups.
3. Conducting personal, for-profit transactions or business or conducting any fundraising activity not specifically sponsored, endorsed, or approved by The City of Scranton.
4. Participating in Internet activities that inhibit an employee's job performance or present a negative image to the public, such as auctions, games, accessing pornographic or offensive material, or any other activity that is prohibited by policy or law.
5. Attempting to test or bypass the security ("hacking" or "cracking") of computing resources or to alter internal or external computer security systems.
6. Participating in or promoting computer sabotage through the intentional introduction of computer viruses, worms or other forms of malware, i.e. malicious software.
7. Promoting, soliciting or participating in any activities that are prohibited by local, state, or federal law.
8. Violating or infringing the rights of any other person.
9. Using any other Authorized User's password and/or equipment to conduct unacceptable activities on Scranton IT Resources.
10. Harassing or threatening activities including, but not limited to, the distribution or solicitation of defamatory, fraudulent, intimidating, abusive, or offensive material.
11. Transmitting or soliciting any proprietary material, such as copyrighted software, publications, audio or video files, as well as trademarks or service marks without the owner's permission.
12. Promoting or participating in any unethical behavior or activities that would discredit The City of Scranton or its departments.
13. Downloading and/or installing any unapproved software.
14. Transmitting or posting any messages that intentionally misrepresent the identity of the sender, hide the identity of the sender, or alter a sender's message.

15. Sending or forwarding confidential or sensitive City of Scranton information through non-Scranton e-mail accounts. Examples of non-Scranton e-mail accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, and e-mail provided by other Internet Service Providers.
16. Sending, forwarding or storing confidential or sensitive City of Scranton information utilizing non-Scranton accredited mobile devices. Examples of mobile devices include, but are not limited to, Personal Data Assistants, two-way pagers and cellular telephones.
17. Participating in any other Internet or E-mail use that is deemed inappropriate by The City of Scranton and/or its departments and is communicated as such to Authorized Users.

Effective 12/29/2008