HUMAN RESOURCE POLICY #32 (ADMIN)

COMPUTER, TECHNOLOGY AND NETWORK USE – EMPLOYEE RIGHTS AND PRIVILEGES

Approved by: **Personnel Board** **3/28/2013** **City Council** **2/25/2014**

Mayor of Omaha: **Jean Stothert**
City Council President: **Pete Festersen**
Human Resource Director: **Michele Frost**

Pursuant to the Omaha Municipal Code, Section 23-65, this document is a Human Resource policy of the City of Omaha. Please check the City's website, http://www.cityofomaha.org/humanresources/public-documents/hr-policies for the latest version of this policy. Where no policy or guideline exists or if there are questions on this policy, please contact the Assistant Human Resources Director/Labor Relations Director in the Human Resources Department.

Purpose:

The purpose of this policy is to set guidelines for users of the City's computers and technology. This policy is designed to balance the trust and responsibility of all users with the complexity and inter-relational aspects of the City computers and technology. Additionally, this policy should serve as a companion with the City's other computer and technology policies and executive orders, including the Social Media and Privacy policies and the Mayor's Executive Order on Cell Phone Usage.

Policy:

A. Definitions

City computer(s): All computer hardware, software, technology, data, networks, programs, systems, and related property, equipment or material from City of Omaha contractors and consultants managed or used by City employees or contractor.

E-mail: Electronic messaging systems.

DOT.Comm: The Douglas-Omaha Technology Commission and any authorized inter-departmental information system/computer units.

User(s): All City employees, contractors, consultants, vendors, interns, volunteers, or permitted operators of the City computers, technology, and/or network.

UserID: A user's login initiation code and any corresponding passwords with that login code.

B. General Guidelines

City computers and technology are the responsibility of the City of Omaha. Users are required to comply with this policy, any applicable user manuals, applicable department/division manuals, and any other directives or policies involving City computers and technology.

Any infraction of this policy, including any action that has brought or might bring public embarrassment to the City, may subject the violator to disciplinary action up to and including termination and possible criminal prosecution. Any behavior or usage of any City computer or technology that violates the concept of basic human dignity in the workplace will not be tolerated. This includes, but is not limited to, the sending or attempted sending of any e-mail or information that is harassing, obscene, and/or threatening to the recipient. All information stored on the City computers and technology will be subject to all other City policies.

City computers and technology are tools to be used by appropriate users. Use of City computers and technology requires the user to employ courtesy, professionalism, and good judgment. No City computer or technology shall be used to play games or other entertainment programs unless approved by the user's supervisor. Should a User desire to use his computer for non-job related activities, he/she must get express consent from his/her supervisor. A supervisor shall approve or deny such a request based upon sound business principles (e.g. length of use, time of use, frequency of use, etc.). Users are responsible for all electronic mail, postings, or materials sent by them, and, as such, all messages should be accurate, appropriate, lawful, and limited to public information. Any attempt to forge, read, delete, copy, or modify the e-mail or Internet/Intranet communication of another user is prohibited. There shall be no use of the e-mail, Internet, or Intranet system to send unsolicited junk mail, "for-profit" messages, chain letters, or any other message that is inappropriate for a business setting or violates City policies. Departmental e-mail bulletin boards shall be governed by internal departmental policies.

Users of City computers and technology are not allowed to attach to any correspondence or e-mail from a City computer any personal "messages", "icons", "symbols" or "quotations", regardless of the content of that message, unless his/her Department Director approves such message, icon, symbol, or quotation. Computers and technology are for City business and no personal (non-City business related) "tags" or "signature messages" are allowed. Employees who have questions regarding this prohibition should not assume any message or quotation is "acceptable" or "appropriate." Any questions regarding attached personal messages, icons, symbols, or quotes should be directed to the City Human Resources Department.

Access to City computers and technology to perform the job duties of the user is considered a privilege. A user should have no expectation of privacy in the use of City computers and technology. All information stored and received on City computers and technology is the property of the City by ownership or license.

Department heads or their designee(s) may apply for service accounts from DOT.Comm for their respective user(s). If DOT.Comm approves such applications, then DOT.Comm will create a service account for the user. Users are responsible for their userIDs. Users should not give their userID or password to anyone or use a userID or password that is not assigned to them unless authorized by DOT.Comm. Any attempt to use someone's userID or password by deceit or fraud or to disguise the identity of the account being used or who is using that account is prohibited.

Passwords are considered unique and confidential to the user and their protection is the responsibility of the user. It is recommended that users avoid writing down passwords for City computer and technology in an unsecured area. The user will be responsible for all activity that occurs under his/her account.

City computers and technology should not be left unattended without first locking or logging out. Failure to lock or log out of a City computer is the responsibility of the user, and, as such, the user shall be held responsible for any actions that occur from his/her unattended City computer, whether the actions were done by the user or not. In addition, often City computers and technology are portable and are used outside of the office. The user is responsible for the maintenance and security of such portable computers and technology, including the data stored therein, when used outside of the typical office setting. Confidential information should not be downloaded or stored on such portable resources unless proper encryption and password protection mechanisms are in place. Any negligent failure to maintain and/or secure such computers and technology, including the data stored therein, could result in a violation of this policy and bring possible disciplinary action against the user.

No user should disclose, circulate, or transmit any City proprietary or confidential information on or with City computers and technology to any unauthorized party. Any breach of confidentiality by a user through the dissemination of City proprietary information will subject that user to disciplinary actions, up to and including termination.

In the event of problems with City computers and technology, users should contact the DOT.Comm service desk unless departmental policy, approved by DOT.Comm, dictates otherwise. Any unauthorized actions that damage or disrupt any City computer or technology, alter the normal performance of City computers or technology, or cause City computers and technology to malfunction are a violation of this policy regardless of the location of the system or the length of time the network system is down.

No user shall run or install on a City computer or technology any software, hardware, or network devices that are not the property of the City of Omaha or DOT.Comm without permission of DOT.Comm. No user should remove from City property programs or software owned by the City or DOT.Comm unless authorized by DOT.Comm. All City computer users are required to abide by the terms of all software licensing agreements and copyright laws. Any copying or making available on City computers and technology of copyrighted materials without permission of the licenser is prohibited.

DOT.Comm must authorize any computer program or software owned by the City to be installed or run on any computer not owned by the City. No computers and technology that are not City property shall be installed in any City offices or attached to any City networks unless authorized by DOT.Comm. Any non-City computers and technology attached to City networks are subject to this policy and, as such, users should remember that they have no expectation of privacy while connected to the City network and all information stored and received on such non-City property could be subject to review.

In summary, there are a number of activities that users can and cannot do with City computers and technology under this policy. Below, are some but not all, of those activities:

- Users must comply with this policy, any applicable user manuals, applicable department/division manuals, and any other directives or policies involving City computers and technology.
- Users must exhibit appropriate behavior, courtesy, professionalism, and good judgment in the usage of any City computer or technology. This encompasses the concept that users avoid any and all activities and deeds that infringe upon self-respect in the workplace.
- Users may not use City computers and technology for non-job related activities, unless given express consent from his/her supervisor.
- Users are responsible for all materials used, sent or received through the City's computer and technology, and, as such, all materials should be accurate, appropriate, business-related, lawful, and limited to public information.
- No user should disclose, circulate, or transmit any City proprietary or confidential information on or with City computers and technology to any unauthorized party.
- No user shall run or install on a City computer or technology any software, hardware, or network devices that are not the property of the City of Omaha or DOT.Comm without permission of DOT.Comm. No user should remove from City property programs or software owned by the City or DOT.Comm unless authorized by DOT.Comm.
- No computers and technology that are not City property shall be installed in any City offices or attached to any City networks unless authorized by DOT.Comm.
- User must not violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations. One example of this would be the unauthorized installation or distribution of "pirated" or other software products that are not appropriately licensed for use by City of Omaha.

- Users are prohibited for the unauthorized copying of copyright 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 of Omaha or the authorized user does not have an active license.

- The exporting of software, technical information, public safety information, or encryption software, in violation of international or regional export control laws, is illegal. The Human Resources Department, the Law Department and/or DOT.Comm should be consulted prior to the export of any material that is in question.

- Users shall not knowingly introduce any malicious programs into the network or servers (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) that may gain unauthorized access to any computer or computing system and cause intentional disruption.

- Use of City computers and technology to actively engage in procuring or transmitting materials in violation of local, state and federal codes and law, including discriminatory, sexual harassment or hostile workplace laws, is prohibited.

- Users may not make fraudulent offers of products, items, or services originating from any City account.

- Users must avoid actions that lead to computer security incidents, disruptions of network communication, port and security scanning, network monitoring, circumventing or disabling security protocols and software, and interfering or denying user service. Security incidents include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly permitted 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.

- Users shall not conduct personal business or practices of any type that are intended for personal gain or misuse the systems for non-City recreational or business purposes. Security software (i.e. firewalls, anti-virus, anti-spyware, etc) shall not be removed or disabled by an authorized user for any reason.

C. Network Access

Users share the City computers and technology every day for a number of services, including file storage and printing capabilities. Deleting, examining, copying, or modifying of files and/or data created by another user without his/her prior consent is prohibited. Any attempt to willfully introduce computer viruses or other disruptive or destructive programs into the City computers and technology is prohibited.

Users have the responsibility to decide which documents, files, and information used by them to maintain and save on City computers and technology. However, users should also be aware that many of the documents, files, and information used by them could be subject to disclosure in litigation, subpoenas, or internal City investigations, or may be required to be stored by a relevant local, state, or federal regulation, statute, or law. Any questions regarding whether materials are required to be stored because of legal reasons should be addressed to the Law Department.

DOT.Comm, as administrator of the network system, will monitor the amount of storing space a user is consuming on the network. A user claiming excessive storage space on the network or saving application software on the network when it should be saved on a local drive is prohibited. Any user questions regarding where materials should be saved or the size and amount of materials saved on the network should be submitted to the user's supervisor and DOT.Comm.

DOT.Comm will have the right to disable any network accounts should systems and resources be viewed as compromised.

D. Electronic Mail

The City provides e-mail for many of its users as a way to facilitate communication.

The e-mail system and all e-mail messages and information retrieved, stored, and sent on or within the City computer network system is always considered to be the property of the City and may be subject to disclosure in litigation, subpoenas, or internal City investigations. Users have no right to privacy or confidentiality in their use of e-mail. The City may periodically, with or without cause or notice, monitor use of e-mail and inspect and read a user's e-mail.

The determination to read or monitor a user's e-mail shall be made by the user's supervisor, DOT.Comm, and the Assistant Human Resources Director/Labor Relations Director. DOT.Comm, in conjunction with a user's supervisor, has the right to recommend removal of a user's e-mail account based on the non-use or inappropriate use of that account. This policy regarding e-mail shall apply both to internal (i.e., City employee to City employee) and external (i.e., City employee to non-City employee) communication.

E. Internet/Intranet

The City provides Internet and Intranet access to many users as a tool to be used in the user's position. The City or its agents will periodically, with or without cause or notice, monitor use of the Internet/Intranet and inspect and read a user's Internet/Intranet records and downloaded materials. The determination to read or monitor a user's Internet/Intranet account shall be made by the user's supervisor and the Assistant Human Resources Director/Labor Relations Director with assistance from DOT.Comm.

Users have no right to privacy or confidentiality in their use of the Internet or Intranet. All users are restricted from any knowing use of the Internet or Intranet to access, download, view, or copy any information that could be considered obscene, derogatory, harassing, inappropriate for the workplace, or in violation of City policies or applicable laws. If a user has any questions about the content or legality of information downloaded, received, or sent by and through the Internet/Intranet, then the user must immediately contact his/her supervisor. Any information a user posts or writes on or over the Internet or Intranet should be professional, accurate, and limited to public information. Any user involved in content generation on the City's official web site or through the Intranet must adhere to the administrative guidelines set by DOT.Comm. Any tampering, defacing, or destruction of information on the City's official web site or through the Internet/Intranet is prohibited.

Department directors reserve the right to limit any user's access to various Internet or Intranet sites that he/she deems inappropriate or not conjunctive to legitimate business purposes. Additionally, directors reserve the right to, at any time, terminate any of their user's Internet or Intranet access.

Users should be on guard against fraud, scams, or viruses. Any improper or questionable information received or intercepted by a user, or any concerns that users have about using their Internet/Intranet access, must be reported to DOT.COMM and the user's supervisor.

F. Remote Login

Supervisors must approve their Users to apply for remote login access with DOT.Comm (See FLSA Compliance Policy). This remote login access may have a fee that will be paid by the department or user applying for this access. Users are required to follow DOT.Comm guidelines for proper network access through a remote login. The use of remote login access is subject to this policy, DOT.Comm guidelines, and all other applicable policies and manuals.