FOR OFFICIAL USE ONLY

City of Buffalo

Department of

Management Information Systems

City of Buffalo Network System [CBNS]

Network Policy & User Agreement

10 December, 2013

CBNS-NetworkPolicy_2013-12-10_Current.doc

FOR OFFICIAL USE ONLY

CONTACTS

Direct any general questions about the Network Policy and User Agreement to your department head. If you have any questions about specific issues, call the following officers:

-Computers and Network Systems
Director of Management Information Systems
(716) 851-4836

-Violations
Commissioner Of Human Resources
(716) 851-4095
Corporation Counsel
(716) 851-4343

DEFINITIONS

These definitions apply to these terms as they are used in this Policy:

City Computers and Network Systems (City Systems):
Computers, networks, servers, and other similar devices that are administered by the City and for which the City is responsible. Throughout this Policy, the shortened term "City Systems" is used to mean City computers and network systems.

Electronic Communications:
The use of computers and network systems in the communicating or posting of information or material by way of electronic mail, bulletin boards, or other such electronic tools.

Electronic Mail (E-Mail):
Network of computer hardware and software that permits the sending and receiving of electronic messages from one personal computer to another.

Internet Access:
The ability for any personal computer to connect to the worldwide network of computers known as the Internet and to access Internet-based applications such as Newsgroups, Gopher, File Transfer Protocol (FTP), Telnet, Wide Area Information Services (WAIS), or the World Wide Web (WWW or web).

LAN Mail Message:
A message sent using City computers or systems to other than named individuals (generally Lanusers).

Network Systems:
Includes video and data networks, switches, routers and storage devices.

Privacy:
The organization respects the individual privacy of its employees. However, employee privacy does not extend to the employee's work-related conduct or to the use of organization-owned equipment or supplies. This includes the components that permit employees to connect to the Internet and to use the e-mail system.

Systems or Network Administrator:
A City of Buffalo employee responsible for managing the operation or operating system environments of computers or network systems, respectively.

I. NETWORK USE

OVERVIEW

Computers and network systems offer useful, productive tools in the modern workplace. These tools also have a recreational and social use in today's society. When used appropriately, these tools can enhance dialog and communications. Unlawful or inappropriate use of these tools, however, can infringe upon the rights of others. While the City of Buffalo recognizes that integrating all uses of computers and network systems in the workplace can increase efficiency and creativity, build morale, and expand access to information, there is also danger of abuse. The City of Buffalo intends to promote responsible use of its computers and network systems in a manner that is consistent with the goals of the City.

The City recognizes the complexity of deciding what constitutes appropriate use of electronic communications services. What is appropriate or inoffensive to some members of the community or workforce may be inappropriate or offensive to others.

Caution: Having open access to network-based services implies some risk. In a community and workforce of diverse cultures, values, and sensitivities, the City cannot protect individuals against the existence or receipt of electronic material that may be offensive to them.

Nevertheless, the City reserves the right to place restrictions on the use of its computers and network systems.

This Policy is in accordance with City policies concerning harassment, applicable work rules and collective bargaining agreement provisions regarding discipline, use of computers and network systems generally, and related statutes. Any restrictive actions by the City pertaining to this Policy will conform to the United States Electronic Communication Privacy Act of 1986.

Caution: A system or network administrator may detect evidence of a violation while performing his or her duties operating or maintaining a system. In such instances, the System or Network Administrator should contact the Commissioner of Human Resources, or the Corporation Counsel for further guidance.

Caution: This policy does not abrogate departmental policies governing the operation and maintenance of City systems provided they do not conflict with the precepts of the City Policy. Departments and divisions may wish to develop ancillary procedures that support organizational requirements (e.g., payroll data entry). Specifically, *procedural guidelines* with regard to security, privacy and other areas of critical importance to the administration of these systems are not addressed as part of this policy.

POLICY SPECIFICS

1. Computers provided by the City of Buffalo for use by employees in the regular course of their duties shall be used for official business only, except that recreational computer network systems use before or after official work hours, or during lunch or break times may be permitted. Such recreational use must be consistent with the provisions of this of this Policy and applicable City policies or Codes, contractual obligations, or state or federal laws and may not endanger the integrity of the City Systems.

2. Software, program downloads and other programs not specifically approved by the System or Network Administrator are prohibited. Approvals should be requested through the Electronic Solution Center Request Program.

3. The City reserves the right to remove or limit access to material posted on the City owned computers when applicable City policies or codes, contractual obligations, or state or federal laws are violated.

4. The City reserves the right to limit access to its computers and network systems when applicable City policies or codes, contractual obligations, or state or federal laws are violated.

5. Union business may be conducted on the City Systems only by designated union officers. The unions shall designate in writing upon promulgation of this Policy and, thereafter, following applicable union elections, to the Commissioner Of Human Resources those union officers to which access may be granted for union business on the City Systems. A union's access shall be for informational purposes only and not for advocacy of issues.

6. Internet access is limited to official, work-related research or communications, except as provided in paragraph 1 hereinabove.

7. Electronic mail may be used for official city-related business, consensual person-to-person communications, and union business or announcements by designated union officers as described in paragraph 5 hereinabove.

8. All electronic mail messages, records of such messages, and City Systems use are subject to monitoring and review by the City at any time. All records of Internet access are also subject to inspection and review by the City at any time.

POLICY VIOLATIONS

1. City computers and network systems may not be used:

a. For private business solicitations;

b. To harass, threaten, or otherwise cause harm to a specific individual whether by direct or indirect references;

c. To impede, interfere with, impair, or otherwise cause harm to work-related activities or data storage;

d. To download or post to City Systems or transport across City Systems, material that is illegal, proprietary, in violation of City contractual obligations, or otherwise is damaging to the City;

e. To send LAN mail message unless such message relates to City business or, for example, to lost items, to an employee's retirement or death;

f . To send other types of LAN mail messages without the consent of the System or Network Administrator and the Commissioner of Human Resources;

g. To download or view pornographic or prurient materials.

2. Violations covered by this Policy include, but are not limited to the following:

a. To refuse to comply with any lawful directive of a clearly identifiable City official acting in the performance of his or her duties in the enforcement of this Policy;

b. To forge, fraudulently alter, or willfully falsify or otherwise misuse City records (including computerized records, permits, licenses, identification cards or other documents or property) or to possess such altered documents;

c. To abuse or threaten another;

d. To steal or knowingly possess stolen property (misappropriation of data or copyrighted materials, including computer software, may constitute theft);

e. To traffic, for profit or otherwise in goods or services when incompatible with the interests of the City;

f. To harass another person. Harassment may encompass but is not limited to sending repeated and unwanted communications by electronic mail;

g. To recklessly or maliciously interfere with or damage computer or network resources or computer data, files or other information;

h. Sending repeated and unwanted (harassing) communication by electronic mail or other electronic communication that is motivated by race, ethnicity, religion, gender, or sexual orientation;

i. Propagating electronic chain mail;

j. Interfering with electronic communications of others by “jamming” or “bombing” electronic mailboxes;

k. Forging, fraudulently altering, or willfully falsifying electronic mall headers, electronic directory information, or other electronic information generated as, maintained as, or otherwise identified as City records in support of electronic communications;

1. Using electronic communications to forge a City document;

m. Using electronic communications to hoard, damage, or otherwise interfere with City resources accessible electronically;

n. Electronically distributing or posting copyrighted material in violation of license restrictions or other contractual agreements;

o. Launching a computer worm, computer virus, malicious code or other rogue program;

p. Downloading, transporting or posting illegal, proprietary or damaging material to a City computer;

q. Using the network in a manner which violates any federal, state or local law.

REPORTING VIOLATIONS

1. If you believe that a violation of this policy has occurred, contact the System or Network Administrator responsible for the system or network involved, who will report the incident to the Director of Management Information Systems , Corporation Counsel, the Department or Division Head, or the Commissioner Of Human Resources in accordance with the applicable procedural guidelines.

2. Anyone who violates this policy will be subject to appropriate disciplinary action. If an employee is a member of a collective bargaining unit, disciplinary action will be taken pursuant to the disciplinary provisions of the applicable collective bargaining agreement.

II. INFORMATION SECURITY

OVERVIEW

The Department of Management Information Systems (M.I.S.) Information Security goals are to minimize the probably of malicious code, viruses and other forms of corruptive code from gaining access to the City of Buffalo Network System (CBNS). M.I.S. also employs several technical strategies to filter inappropriate http / https (Internet) and SMTP (e-mail) content. The department has also taken steps to prevent unauthorized physical access to CBNS servers, communications and corporate printing equipment.

The Department of Management Information Systems (M.I.S.) will continue to develop and modify Information & Network security policy, guidelines, standards, procedures and controls with regard to the use and maintenance of the City of Buffalo Network System in response to changing technologies and functional application.

At present the Department of Management Information Systems provides several layers of security for the City of Buffalo Network System.

SECURITY ZONES AND LEVELS OF TRUST

The Department of Management Information Systems has established and will maintain two broad security zones, secure and unsecured from external malicious activity emanating from the Internet. As M.I.S. expands its network security architecture additional security zones will be established providing varying levels of security within the CBNS.

PHYSICAL SECURITY AND ACCESS CONTROL

The Department of Management Information Systems has established and will maintain physical security and access control to the operations room located in M.I.S. access to communications rooms and lockers are under the asepses of the Department of Public Works. The physical security systems for M.I.S. spaces includes programmable magnetic keys to manage time of access and provide for entry and exist auditing; cipher locks and audiovisual equipment for monitoring the environment outside of the operations room and both entries to M.I.S. spaces.

FIREWALL

The Department of Management Information Systems has established and will maintain a firewall that stands between the CBNS and its DMZ and direct connection with the Internet. Firewall capabilities and logs provide for several layers of defense against malicious code, unauthorized entry, unauthorized protocols and auditing functionality. M.I.S. personnel will maintain this capability. The department is in the process of enhancing that defense by developing a secondary firewall.

WEB FILTERING

The Department of Management Information Systems (M.I.S.) has established and will maintain an http / https filter capability to mitigate the risk of exposure of users to inappropriate web content and to prevent access to sites that have been deemed as inappropriate. Recognizing complexity in determining what constitutes a content appropriate site, and the technical challenges to restrict access to web sites that contain inappropriate content the M.I.S. has contracted with private industry specializing in analyzing, codifying and controlling web content access and providing services to filter web traffic and block accessibility to certain web sites. The City has selected certain categories of web sites that these services should block; the service company and related technology then acts to block all traffic that belongs to that category. The City has selected many categories to be blocked, including adult web sites and porn web sites. Private industrial services describe adult web sites as sites that contain images of nude men or women; adult dating services or single listings with sexual images or content; escort services or strip clubs; sexual enhancement products or techniques; buying, selling, or distributing sex toys, sex videos, or other sex related products; and groups or forums focused on sexual objects. Private industrial services describe porn web sites as sites that contain images or video of sexual acts or fetishes; explicit cartoons and animation featuring sex acts, descriptions or stories of sexual acts or fetishes; and child pornography/ pedophilia. As part of the contracted service to the City of Buffalo, the service provider reviews the content of a site to determine how the site should be categorized. The City is not aware of the criteria the service provider uses to categorize web sites. In some cases the service provider blocks sites that are necessary to the performance of an employee's job. In such cases, the Management Information Systems department may unblock access to a particular site provided the employee identifies a legitimate business related purpose for access to that site. M.I.S. personnel will maintain this capability.

VIRUS SCANNING/BLOCKING SOFTWARE

The Department of Management Information Systems has implemented and will maintain the use of interior network virus scanning software, specifically focused on the e-mail Exchange server. The software inspects, identifies and isolates or removes files matching known malicious code signatures. M.I.S. personnel will maintain this capability.

E-MAIL FILTERING

The Department of Management Information Systems has established and will maintain an SMTP filter capability to mitigate the risk of exposure of users to inappropriate e-mail content and manage traffic on the CBNS. M.I.S. personnel will maintain this capability.

INTRUSION DETECTION SYSTEM

The Department of Management Information Systems has established and will maintain Intrusion Detection System (IDS) capabilities. The IDS sensors will be directed toward external intrusion activities to provide a method of exposing external attempts to probe, hack and exploit any possible gaps in the CBNS defenses. M.I.S. will also continue to expand its present IDS capabilities as budget and manpower constrains allow. M.I.S. personnel will maintain this capability.

DESKTOP SYSTEM SECURITY FEATURES

The Department of Management Information Systems has established and will maintain Desktop security features that protect against various malicious codes, viruses, sypware, ad-ware and pop-ups at the desktop environment. As new signatures for malicious code and viruses are discovered and distributed Users are provided with and informed of available updates. Users are required to update their desktop security application engines and definitions as directed by the Department of Management Information Systems.

PASSWORDS

- Minimum length: 8 characters
- Complexity: must contain characters from at least three of the following four categories:
    - Upper case letters
    - Lower case letters
    - Numbers
    - Special characters (e.g.:$, #, or punctuation characters such as ? !).
- Maximum password age: 90 days
- Are NOT to be divulged to any other individuals

The most widely used computer authentication security and control technique involves the use of confidential character strings known as passwords, user IDs, and security codes, terms that are used interchangeably by most people. A password can be defined as any character string intended to remain confidential and used to control access by individuals to computer resources, including data, equipment, communication links and software. The minimum length of a CBNS password is 8 characters. Complexity requires a combination of at least three of the categories listed above.

Passwords are a pervasive aspect of computer security. The effectiveness of using passwords to restrict and control access is based on limiting knowledge of the password to an individual user. Users are responsible to take appropriate steps to insure the confidentiality of CBNS passwords.

The frequency of password change impacts confidentiality. The chance of disclosure increases over time. Passwords can become common knowledge in the workplace if not frequently changed. Users will periodically change passwords in order to protect confidentiality. The CBNS will require password changes at a minimum of every 90 days, users will be notified daily of the required password change beginning 10 days prior to password expiration. A password history will be maintained to limit reuse of previous passwords. A valid password can not be a password that has been used for any one of the previous 6 passwords.

PASSWORD DISTRIBUTION & MAINTENANCE

Telephone contact for distribution and maintenance of passwords is authorized.

M.I.S. personnel and Users may control password changes.

Users will receive separate passwords for access to Virtual Private Networks (VPNs)

USER LOGIN IDs

A user login ID [LID] is the user individual account identifier; each user account carries with it several properties ranging from specific login scripting, e-mail addresses and authorized resource access to hours of authorized operation. To protect both personal information on the local work station (PC / host computer) and CBNS resources and resident CBNS information users are required to:

- Complete, sign and forward to M.I.S. the ACKNOWLEDGEMENT OF RECEIPT BY EMPLOYEES form at the end of this document
- Lock their work station when they leave the immediate area (control-Alt-Delete – Lock Computer)
- Never grant use of their LID to another individual
- Never employ another CBNS user LID to gain access to the CBNS

Note: To conserver limited system resources and prevent unauthorized access User Login accounts that are **Inactive for a period greater than 120 days are subject to deletion** without notice at the discretion of the Department of Management Information Systems.

NETWORK ADIMINISTRATIVE CREDENTIALS

Some CBNS account holders may be granted enhanced credentials for additional access not granted routine CBNS users in support of local departmental or City enterprise wide operations. The additional access may be temporary or of a more permanent nature as determined by departmental and enterprise wide requirements, restrains and operational tempo. Additional access may be granted and revoked by appropriate M.I.S. personnel. Additional access requires additional responsibility for the security the City of Buffalo Network System. Should enhanced credentials be revoked due to violations of the CBNS Network Policy and User Agreement or Federal and New York State Consolidate Laws as listed in this Network Policy and User Agreement or any other Computer regulatory Law enacted by Federal, State, County or City of Buffalo authorities, reinstatement of any additional access or enhanced credentials will require a written request by elected or appointed senior city leadership (I.e. Mayor, Deputy Mayor, appointed department Commissioner) and approval of the Commissioner of the Department of Management Information Systems.

SECURITY AWARENESS

For the purpose of familiarizing users with the CBNS Information Security policy and educating users on recommended practices, the Department of Management Information Systems has established and will maintain a regularly published informational newsletter; an organized users group and departmental policy.

Practices promulgated include but are not limited to:

- Educating users on the creation of good passwords
- Do's and don'ts for maintaining workstations
- Informing users of e-mail and Internet access policies
- Employee responsibility for computer security
- Incident reporting procedures
- How to identify social engineering tactics
- Protecting information

The main purpose of the Information Security Policy is to inform users, staff and managers of their obligatory requirements for protecting technology and information assets. The policy specifies the mechanisms through which these requirements can be met. It is also to provide a baseline from which to acquire, configure and audit computer systems and networks for compliance with the policy.

INCIDENT REPORTING

The Department of Management Information Systems has in the past reported computer incidents and will continue to report computer incidents to the Federal Computer Incident Response Center (**FedCIRC**) and the National Infrastructure Protection Center (**NIPC**) via United States Computer Emergency Response Team (**US-CERT**). FedCIRC is part of the National Cyber Security Division (NCSD), a division of the Information Analysis and infrastructure Protection (IAIP) Directorate in the Department of Homeland Security(DHS). US-CERT is a partnership between the Department of Homeland Security and the public and private sectors. Established to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation.

COMPUTER CRIME INVESTIGATION

The FBI has implemented various technical programs to address the growing complexity of computer investigations. In Washington, D.C., the National Infrastructure Protection Center (NIPC) (formerly part of the FBI) is a special unit of the Department of Homeland Security that coordinates computer crime investigations throughout the United States. The DHS trains and certifies computer forensic examiners for field offices in the United States to recover and

preserve digital evidence. The DHS maintains a computer forensic laboratory in Washington, D.C., for advanced data recovery and research and development.

Computer crimes can be separated into two categories:

- Crimes facilitated by a computer
- Crimes where the computer is the target

Computer-facilitated crime occurs when a computer is used as a tool to aid criminal activity. This can include storing records of fraud, producing false identification, reproducing and distributing copyrighted material, and collecting and distributing child pornography, among others. Crimes where computers are the targets are related to activities that damage the targeted host, network or data.

COMPUTER CRIME LAWS

In 1984, Congress adopted the view that computer crime cannot be analogized to traditional crime and that combating it requires both innovative law enforcement techniques and new laws designed to address abuses of emerging technologies. Some computer offenses are based on new technologies and must be specifically addressed by statute. A criminal seeking information stored in a networked computer with dial-in access can acquire that information from virtually anywhere in the world. The quantity of information stolen or the amount of damage caused by malicious programming code may be limited only by the speed of the network and the criminal's computer equipment. Moreover, such conduct can easily occur across state and national borders.

Several federal laws have been developed to address computer crime. The major federal and New York state computer security laws and regulations at the time of this writing include:

- Privacy and Security Act of 1974
- Foreign Corrupt Practices Act of 1977
- Electronic Fund Transfer Act of 1978
- Right to Financial Privacy Act of 1978
- Computer Fraud and Abuse Act of 1984
- Small Business Computer Crime Prevention Act of 1984
- Computer Fraud and Abuse Act of 1986
- Electronic Communications Privacy Act of 1986
- Computer Security Act of 1987
- National Information Infrastructure Protection Act of 1996

- New York State Consolidated Laws Article 156
  - Section 156.00 Offenses involving computers; definition of terms.
    156.05 Unauthorized use of a computer.
    156.10 Computer trespass.
    156.20 Computer tampering in the fourth degree.
    156.25 Computer tampering in the third degree.
    156.26 Computer tampering in the second degree.
    156.27 Computer tampering in the first degree.
    156.30 Unlawful duplication of computer related material.
    156.35 Criminal possession of computer related material.
    156.50 Offenses involving computers; defenses.

Based on the defendant's authority to access the computer and criminal intent to damage the chart below lists present categorization of computer criminal activities.

1. Description	Trespassers	Authorized Users
Intentional Damage	Felony	Felony
Reckless Damage	Felony	No crime
Negligent Damage	Misdemeanor	No crime

This page intentionally left blank

ACKNOWLEDGEMENT OF RECEIPT BY EMPLOYEES

I acknowledge receipt of the City of Buffalo Network Policy and User Agreement.

Signed:_____

Title:_____

Department:_____

Date:_____

A copy of this agreement will be kept on file with System or Network Administrator charged with issuing your computer access.