TOWN OF EAST HARTFORD
INFORMATION SYSTEMS USE POLICY

The Town of East Hartford maintains an Information Systems Use Policy. The policy establishes rules of conduct for use of all of the Town of East Hartford's Information Systems. It is very important for you to understand that these policies are in effect.

TOWN OF EAST HARTFORD
INFORMATION SYSTEMS USE POLICY

PURPOSE:

To establish rules of conduct for use of all Town of East Hartford Information Systems, including but not limited to, telephone (land line and cellular), voice mail, facsimile machines, computers, electronic mail, Internet access, and network access privileges provided by the Town of East Hartford (the "Town of East Hartford Information Systems" or "Town's Information Systems"). This policy applies to the use of Town of East Hartford Information Systems at all locations. Town of East Hartford Information Systems covered by this policy include those that are entirely owned and operated by the Town of East Hartford. Town of East Hartford Information Systems shall also include information system(s) or applications(s) owned by third parties and utilized by the Town or any of its employees or agents.

Officials and employees of the town, wherever situated, should at all times be aware that the Town of East Hartford reserves the right to monitor for any purpose email messages, Internet use, other electronic files created by employees and all other components of the Town's Information Systems to ensure compliance with this policy. Telephone use may also be monitored on a user-by-user basis for appropriate cost controls. Random monitoring may be conducted in addition to any specific monitoring deemed necessary by upper management. The Town's Information Systems may be monitored by using computers, and/or telephones, wires, cameras, electromagnetic, photo-electronic or photo-optical systems. The posting of this notice constitutes the prior written notice required by section (b) (1) of Connecticut General Statute 31-48d. No further notice will be given.

At no time shall the Town of East Hartford's Information Systems be used outside the scope of the provisions of these polices. These policies are implemented to protect the Town of East Hartford, its employees and our systems from damage and liability.

CONDITIONS TO AUTHORIZATION:

Employees are authorized to use the Town of East Hartford's Information Systems as assigned and in accordance with the terms and conditions of this Information Systems Use Policy. If an employee violates this policy, the employee's authorization is deemed to be immediately revoked, without notice.

TOWN OF EAST HARTFORD
INFORMATION SYSTEMS USE POLICY

An employee's authorization to use the Town of East Hartford's Information Systems is contingent on his or her continued compliance with all conditions.

USE:

The Town of East Hartford's Information Systems are carefully managed to allow employees access to resources needed to carry out the business of the Town of East Hartford. This access is maintained to comply with security policy best practices and Town, State and Federal regulations and laws.

PASSWORDS:

For security, passwords will be required to be changed on a regular basis. The Town of East Hartford's Information Systems shall use and enforce the following secure password attributes:

Passwords shall be a minimum length of eight (8) characters.
Passwords shall not be a dictionary word or proper name.
Passwords and Usernames shall not be the same.
Passwords shall not be older than 90 days.
Passwords, if written down, shall not be kept in plain sight.
Passwords shall not be transmitted in clear text outside the Town's Information Systems.

Password change notifications will be automated by the Town's Information Systems. Ample warning of an expiring password will be given.

Password sharing between members of the Town of East Hartford is strictly prohibited. In no event will any personnel give their password to anyone else in order to counter the security measures in place on the network. No individual shall access any Town of East Hartford Information System with any account, logon, username or password, other than that which was issued them by the appropriate systems administrator. Use of another individual's credentials to access any Information System is strictly prohibited. Such actions undermine the overall security and integrity of the network and its data. The exception is action taken under the direction of a System's) Administrator in order to troubleshoot or maintain a system. Also, files may be shared by copying them to an area that is shared on the network for access by multiple users.

In the event that any person needs a change in access to network resources, programs, or data, such will be obtained through proper application for that access through the chain of command. Within one business day after written approval is received from the appropriate authority, the Systems Administrator will grant the approved user the appropriate access rights for their job function.

EXCESSIVE USE:

Users must avoid excessive use of the Town's Information Systems. Excessive use means use that is disproportionate to that of other users, or is unrelated to Town-related needs, or that interfere with other authorized uses. The reasonableness of any specific use shall be determined by the System Administrator or Department Head, in the context of relevant circumstances.

EMAIL:

Officials and employees of the town, wherever situated, should at all times be aware that the town has the ability and right to monitor messages sent and / or received via voice mail and / or electronic mail (e-mail). See "MONITORING" in this policy..

The Town of East Hartford's email system is to be used for conducting the business of the Town of East Hartford. The email system cannot be used to transmit, access, or download offensive, fraudulent, or defamatory images or text, including but not limited to pornography, off-color jokes, discriminatory materials or anything that may be construed as harassing or offensive to others at any time.

The email system cannot be used, at any time, for chatting, sending or propagating jokes, or creating or responding to chain mail or SPAM.

Occasionally "Read Receipts" are requested in response to an email. Any prompts for read receipts, from any employee of the Town of East Hartford, shall not be denied. Read receipts are a useful business tool which aid in management and accountability for all.

E-mail requires extensive network capacity. Sending unnecessary e-mail, or not exercising constraint when sending large files, or sending to a large number of recipients consumes network resources that are needed for critical Town business. When the Town of East Hartford grants an individual employee access to the network, it is the responsibility of the employee to be cognizant and respectful of network resources.

When sending or replying to email - make sure you are sending to an individual when you want to send to an individual and a group when you want to send to a group. It is best to address directly to an individual(s) or sender(s). Check carefully, the "To" and "From" before sending mail. It can prevent unintentional errors. Emailing large distribution lists (i.e., Town Hall Personnel, Police Department Personnel and Fire Department Personnel) are strictly reserved for business use and only with the approval of the System Administrator or your Department Head.

"Excessive Use" of the email system shall not be permitted. (See excessive use defined above).

The Town of East Hartford's email system employs a content filter and virus scanner to protect the system and it's users from inappropriate material and/or viruses. Should a

valid email be blocked or quarantined, notify your supervisor or system administrator and an attempt to recover the email will be made.

Avoid opening any email attachment you receive unless the attachment is business related, is clearly identified, and you expected it from the sender. Do not click on web links (URL's) unless the link is business related, is clearly identified, and you expect it from the sender. When in doubt, contact the sender by phone to verify the source and content of attachments or links before you open or click on them. Delete any email containing attachments or links which are from unknown sources or which can not be verified by the sender.

When sending an attachment to an email you are preparing, include a description of the attachment content, including the file name and approximate file size and attempt to notify the recipient of your pending delivery. Should you have any reason to believe your PC has been infected by a virus, notify your system administrator immediately.

Despite the existence of any passwords, employees should not assume that any electronic communication is private. It is not and can be monitored at any time without further notice.

Be aware; MAIL ON THE INTERNET IS NOT SECURE. Never include in an email message anything that you want to keep private and confidential because email is sent unencrypted and is easily read. In some circumstances, e-mail may be subject to disclosure in court or administrative proceedings or under Freedom of Information laws.

Be aware if you send anything but plain ASCII text as email. Recipients may not have the ability to open your documents (i.e., Word or VISO documents).

You may want to include a signature (an identifier that automatically appends to your e-mail message) that contains the method(s) by which others can contact you. (Usually your e-mail, address, phone number, fax number, etc.)

For important items, you may want to let senders know you have received their e-mail, even if you cannot respond in depth immediately. They need to know their e-mail is not lost.

INTERNET:

Officials and employees of the town, wherever situated, should at all times be aware that the town has the ability and right to monitor Internet usage. See "MONITORING" in this policy.

Access to the Internet is provided to enhance your capability to perform your Town responsibilities, so its use is permitted strictly and solely for use related to job function. Improper use of this facility will result in Internet service removal and possible

disciplinary action. Town of East Hartford computers are the property of the Town of East Hartford and must not be used for any prohibited purposes.

"Excessive Use" of Internet access shall not be permitted. (See excessive use defined above).

The Town of East Hartford's Internet Access system employs a content filter and virus scanner to protect the system and it's users from inappropriate material and/or viruses. Should a valid web site be blocked, notify your supervisor or system administrator and if appropriate, the access will be arranged.

Town staff requiring Internet accesses as a part of their job function and normal duties shall be provided access, upon request to designated Systems Administrator(s) and Department Heads.

All department heads will be provided full Internet access privileges.

Employees will be provided Internet access privileges based on business needs. Requests for Internet access should be brought to your supervisor detailing demonstrated need. If approved by the supervisor, the supervisor will submit the request to their system administrator. Access will then be issued if network resources allow.

Additional staff may be granted expanded Internet access rights upon request to the designated system administrator(s) and subsequent approval by the Mayor. All requests should identify a strong need for the expanded access and sound reason(s) why access cannot be gained by use of the department head's system. For example, a remote physical location may make use of the Department Head's system impractical.

Visiting pornographic sites, or viewing pornographic materials, on the Town's Internet System is prohibited and will result in discipline or termination. Accidental access to an adult, gaming or otherwise inappropriate site should immediately be reported to their designated Systems Administrator(s) so that all links to the sites may be removed from the computer.

The Town Internet system should not be used for visiting unauthorized sites, except where access to such site is used with prior system administrator approval for research purposes.

The downloading or passing along of offensive materials will result in discipline or termination.

No one may download software from an outside source without prior approval from their system administrator.

HARDWARE:

TOWN OF EAST HARTFORD
INFORMATION SYSTEMS USE POLICY

No one may tamper with, install, or remove any computer, network device, equipment, hardware, wiring, etc. connected to any of the Town of East Hartford's Information Systems without the approval from their systems administrator. No one will install any computer, network device, equipment, hardware, wiring, etc. without the approval and assistance of their systems administrator.

SOFTWARE:

No one may uninstall, disable or interfere with any program or utility running on any of the Town of East Hartford's Information Systems without prior authorization from their systems administrator.

To prevent contamination of the Information System, no employee may download or install software from any source without prior authorization from the Systems Administrator. Any and all software loaded on any computer must be registered to the Town of East Hartford and is the sole property of the Town of East Hartford. Authorization may be obtained by contacting the Systems Administrator. (See Software Piracy and the Law, attached.)

ELECTRONIC FILES:

All users should be aware that any electronic file created on the Town of East Hartford system can be restored and viewed as necessary. For this reason, no Town of East Hartford computer may be used for the creation of a type of file that has been prohibited from viewing in any other part of the system.

REMOVABLE MEDIA:

Be aware that any removable media (floppy disks, CDROM's, DVD's, USB drives, etc.) may contain viruses. Use of any removable media must be approved by your system administrator.

TELEPHONE, FACSIMILE AND VOICE-MAIL:

Prohibitions on Internet and e-mail services such as use of inappropriate language, access to pornographic sites, and use for personal commercial endeavors also apply to the use of the telephone system, facsimile system, voice mail system and all other systems considered by the Town to be part of the Town of East Hartford's Information Systems.

MONITORING:

The Town of East Hartford may monitor e-mail messages, Internet use. electronic files created by employees and all other components of the Town's Information Systems to ensure compliance with this policy. Telephone use may also be monitored on a user-by-user basis for appropriate cost controls. Random monitoring may be conducted in addition to any specific monitoring deemed

necessary by upper management. The Town of East Hartford's Information Systems may be monitored by using computers, and/or telephones, wires, cameras, electromagnetic, photo-electric or photo optical systems. The posting of this notice constitutes the prior written notice required by Section (b)(i) of Connecticut General Statutes Section 31-48(d). No further notice will be given.

HARASSMENT:

The Town's Information Systems may not be used for transmitting, retrieving, or storing any communications of a harassing nature or materials that are pornographic, obscene or X-rated. Harassment of any kind is prohibited. The Town's harassment policy applies in full to all of the Town of East Hartford's Information Systems.

DISCRIMINATION:

The Town of East Hartford's Information Systems may not be used for creating, transmitting, retrieving or storing any communications of a discriminatory nature. The Town's discrimination policy applies in full to all of the Town of East Hartford's Information Systems.

DEFAMATION:

Any messages or information sent by an employee to another individual within or outside the Town via the Town e-mail or Internet systems (including bulletin boards, online services or Internet sites) are statements that reflect on the Town. Therefore, any communication defaming another person, group or organization is strictly prohibited.

COPYRIGHT AND TRADEMARK:

Employees may not transmit copy, retrieve or forward copyrighted or trademarked material that does not belong to the Town using the Town's e-mail or Internet system. Every employee who obtains access to other companies' or individuals' materials must respect all copyrights and trademarks and may not copy, retrieve, modify or forward copyrighted or trademarked materials, except with written permission of the copyright or trademark holder.

CONFIDENTIAL BUSINESS INFORMATION:

All communications sent by employees via the Town's e-mail or Internet system may not disclose any confidential or proprietary information. With proper permission from management, employees may send selected information in an encrypted form. Any encryption programs must be approved by the Town of East Hartford.

UNWANTED CORRESPONDENCE:

If an employee receives unsolicited e-mail from outside the Town that appears to violate the Town's policy, the employee should notify his or her supervisor immediately.

PHYSICAL SECURITY:

Proximity Card Readers are installed at various Town facilities within the Town of East Hartford. These devices provide a higher degree of physical security and accountability to more sensitive locations. Employees shall use their Proximity Card to access any areas secured by Proximity Card Readers.

Use of a key to "bypass" the Proximity Card Reader is prohibited, with the exception of emergencies. Use of a key to bypass a reader must be reported to your supervisor with explanation of emergency. The notified supervisor shall document the emergency and advise their Division/Department Head.

NETWORK SECURITY:

The data on our network represents a substantial investment in labor and dollars and is to be protected at all times. These security policies are in effect in order to preserve the integrity of our data.

USER RESPONSIBILITY:

User responsibility refers to the obligation of the end user to immediately inform their designated system administrator(s) whenever they accidentally encounter a possible "security flaw" or "access risk" to the network; for example, a user having the ability to access another users account, or access data they know they have no authority to access.

SYSTEM BACKUPS:

Daily backups are performed in order to protect the data. The Systems Administrator(s) will set a schedule for such backups in order to preserve and protect the data as is reasonable while minimizing interference with users' regular work schedule as much as possible.

VENDORS/CONTRACTORS:

All vendors or contractors requiring access to the Town of East Hartford's Information Systems shall be referred to the particular department's System Administrator. The System Administrator will assure that the vendors' hardware, software or network access are of secure design and cause no unnecessary security issues.

OUTSIDE AGENCY SYSTEMS:

TOWN OF EAST HARTFORD
INFORMATION SYSTEMS USE POLICY

The Town of East Hartford's Information Systems Use Policy governs employees use for accessing an outside Agency's system. The user shall also follow the policies and guidelines of the outside Agency as trained or certified while accessing that resource.

Outside Agency Applications Include:

POLICE DEPARTMENT

CROG

CAPTAIN/Bluelink

-Requires training.

-Guaranteed messages need supervisor approval (to be documented in the message).

PSA

-Requires training.

COLLECT

NCIC

NLETS

SPBI

FIREARMS

- No Internet web or email access on COLLECT device.
- Requires training and certification.

CJIS

OBTS

- No web browser or email application open concurrently with OBTS application on device.
- Any print out to be pre-approved by a supervisor.
- Requires training and certification.

Cogent Livescan

- Requires training.

HEALTH DEPARTMENT

Connecticut Immunization Registry (CIRTS)

Training

Restricted access privileges (HIPPA)

URS (HIV Tracking)

Training

Restricted access privileges (HIPPA)

REGISTRARS OF VOTERS

ConnVERSE (Connecticut Voter Registry)
Training
Restricted Access privileges limited by physical bandwidth to the registry.

TOWN CLERK

ConnVerse (see Registrars of Voters)

Connecticut Vital Records Registry
Training
Restricted access privileges

VIOLATIONS:

Any employee who violates these rules or otherwise abuses the privilege of the Town of East Hartford's Information System will be subject to corrective and/or disciplinary action up to and including termination. All employees are subject to Connecticut General Statutes, 53a-251 through 53a-256 and any other law or regulations concerning computer crime.

Employees who violate this policy may be subject to disciplinary action up to and including discharge.

GLOSSARY:

Pornographic: any content that is obscene or is intended to excite lascivious feelings. This includes subject matter dealing with any type of sexual act, human or animal and includes all types of communications.

Discriminatory: any statement, message image or content used to denigrate or demean another human being by reason of race, creed, religion, national origin, gender, sexual orientation, age or disability.

Malware: (for "malicious software") is any program or file that is harmful to a computer user. Thus, malware includes computer viruses, worms, Trojan horses, and also spyware, programming that gathers information about a computer user without permission.

Systems Administrator (SA): Designated System Administrator(s) are responsible for protecting and facilitating the Information Systems of the Town of East Hartford and thus for developing and adjusting Information Policies and Procedures as needed. The primary goal is to provide optimum security balanced with ease of use as much as

possible, implementing new technologies and techniques when reasonable. The SA has the authority to make the necessary decisions on security, configuration, implementation and policies and procedures based on his/her technical expertise.

SOFTWARE PIRACY AND THE LAW

Software Piracy in the United States

(Source of this information is the Business Software Alliance)

What Is the Law Regarding Software Piracy?

Most people would never consider stealing something that did not belong to them. But those who copy software without authorization are, in fact, stealing someone else's property — their intellectual property. And, they are breaking the law.

Software development involves a team effort that blends the creative ideas and talents of programmers, writers and graphic artists. And like most creative works, such as books, music and films, computer software is protected by U.S. copyright laws, U.S. code Title 17 and 18.

When you purchase software, you do not become the owner of the copyright. Rather, you are purchasing the right to use the software under certain restrictions imposed by the copyright owner, typically the software publisher. These rules are described in the documentation accompanying the software — the license. Most often, it states that you have the right to load the software onto a single computer and make one backup copy. If you copy, distribute or install the software in ways that the license prohibits, whether you are swapping disks with friends and coworkers or participating in widespread duplication, you are violating federal copyright law. Even if you only help someone else make unauthorized copies, you are still liable under the copyright law.

Many businesses, both large and small, face serious legal risks because of software piracy. Under the law, a company can be held liable for its employees' actions. If an employee installs unauthorized software copies on company computers or acquires illegal software through the Internet, the company can be sued for copyright infringement. This is true — even if the company's management was unaware of the employee's actions.

To make or download unauthorized copies of software is to break the law, no matter how many copies are involved. Whether you are casually making a few copies for friends, loaning disks, distributing and/or downloading pirated software via the Internet, or buying a single software program and then installing it on 100 company computers, you are committing a copyright infringement. It doesn't matter if you are doing it to make money or not — you are exposing yourself to serious civil and potentially even criminal penalties. For example, individuals using the Internet to sell or distribute pirated or counterfeit software programs through online auctions and "warez" sites may be criminally prosecuted, even if they do not profit from the illegal activity.

What Are the Penalties for Pirating Software?

Software theft is stealing. If you or your company would be caught copying software, you may be held liable under both civil and criminal law.

If the copyright owner brings a civil action against you, the owner can seek to stop you from using its software immediately and can also request monetary damages. The copyright owner may choose between actual damages, which includes the amount it has lost because of your infringement as well as any profits attributable to the infringement and statutory damages, which can be as much as $150,000 for each program copied. In addition, the government can criminally prosecute you for copyright infringement. If convicted, you can be fined up to $250,000, or sentenced to jail for up to five years, or both.

In addition to legal consequences, using copied or counterfeit software also means:
• Greater exposure to software viruses, corrupt disks or otherwise defective software
• Inadequate or no documentation and no warranties
• Lack of technical product support available to properly licensed users
• Ineligibility for software upgrades offered to properly licensed users

What Are Your Responsibilities As a Software User?

Your first responsibility is to purchase only legitimate software products. Make sure you get genuine disks, manuals and license documentation. Avoid loose or hand-labeled disks or software offered at prices that are “too good to be true.” Be wary of unscrupulous Internet vendors, who advertise attractive deals on “genuine” software that was overstocked or otherwise discounted for inventory reasons. Remember that a high percentage of software sold on online auctions is illegal.

Next, install and use your software in accordance with the license agreement. Since these agreements differ from publisher to publisher, you need to read them carefully. When someone else installs the software, be sure that individual provides you with proof that the product is fully licensed. If you have outsourced your information technology needs to a consultant or application service provider, you are still responsible for compliance. Software piracy is not a victimless crime. Piracy denies the software developer its rightful revenue and harms consumers and the industry as a whole.

All software developers, both big and small, spend years creating software. A portion of every dollar spent in purchasing original software is funneled back into research and development, so that newer, more advanced software can be produced. When you purchase illegal or counterfeit copies, your money goes straight into the pockets of software pirates.

What Is the Economic Impact of Software Piracy?

In the United States, 22 percent of all computer software is unlicensed. The Business Software Alliance (BSA) estimates that in 2003 the industry lost $6.5 billion in revenue in the United States alone due to software theft. But software piracy’s damaging

economic impact is not only confined to the software industry. In fact, software piracy has an effect on the economic health of the nation as a whole, including jobs, wage and tax revenue losses.

What More Can You Do to Prevent Piracy?

For more information about software piracy, to obtain a free software management guide or to report piracy, call the toll-free BSA antipiracy hotline at 1-888-NO-PIRACY or log on at www.bsa.org.

Business Software Alliance
1150 18th Street, NW
Suite 700
Washington, DC 20036
www.bsa.org

Updated & Revised by Sergeant Gary Willett - EHPD
Revised by Attorney Richard Gentile - Assistant Corporation Council
06/18/2005