TOWN OF EAST WINDSOR COMPUTER/NETWORK ACCEPTABLE USE POLICY

Chapter: 13 – General Management
Section: 4 – Use of Computer Resources
Issue Date: 3/30/2009
Effective Date: 3/30/2009
Amends:
Review: Annual
Authorized –First Selectman

I. Policy

The Town of East Windsor Connecticut relies heavily upon internal and external electronic hardware and software information systems used to efficiently store, retrieve and process information. The security, reliability and integrity of the computer resources and the information networks are of vital importance to the continued successful operation of the Town of East Windsor, herein referred to as town.

This policy addresses all employee use of the town's computer hardware, software and electronic mail systems. The availability and use of personal computers within the work environment have provided many opportunities for enhancement of productivity and effectiveness. However, if not properly managed or used, these technologies can also have a damaging effect on the town, its

employees, and the public. Therefore, all town employees shall abide by the requirements set forth herein when using town's computers, the services of both internal and external databases, law enforcement networks, and the town's electronic mail system.

All employees shall first read this policy and then detach and sign the acknowledgment page at the conclusion of this document. The signed acknowledgment page of the policy is to be retained in each member's employment file.

II. Purpose

To establish rules and regulations designed to promote the effective and responsible use of the Town's computer resources.

III. Scope

This policy applies to all employees (hereinafter referred to as "users") who access or use the computer hardware, software and electronic mail resources provided by the Town of East Windsor.

IV. Definitions:

The following words and terms, whenever used or referred to in this manual, shall have the following respective meanings:

ACCESS: means to instruct, communicate with, store data in, or retrieve data from a computer, computer system or computer network.

APPLICATION PASSWORD: a password that a user may assign within an application and/or document in a town computer that prohibits other users from opening the secured application or document.

AUTHORIZED SOFTWARE: means computer software developed, approved, purchased or licensed by an agency of the Town of East Windsor.

COMPUTER NETWORK: means either a set of related devices connected to a computer by communications facilities, or a complex of two or more computers, including related devices, connected by communications facilities.

COMPUTER SOFTWARE: means one or more computer programs, existing in any form, instructions, manuals, associated operational procedures, or other documentation. Software provides the instructions and controls through symbolic languages of the operation of all computers, including stand-alone and LAN (local area network) computers and related equipment as well as midrange computers.

COMPUTER SYSTEM: means one or more connected or unconnected computers, peripheral devices, software, data, programs, communications facilities, and computer networks.

COMPUTER VIRUS: means a software executable code segment that is covertly incorporated into the executable program code files or data files of a computer or computer network and is activated when the host program executes. It can cause system degradation, including crashes, changes of data or complete erasure of hard drives.

COPYRIGHT: means the rights granted to the owner of software by the Copyright Act, Title 17 of the U.S. Code.

DIRECTORY: a directory is a named group of related files that are separated by the naming convention from other groups of files.

DISTRIBUTION DISK: the original program diskettes, CD's, and DVD's that are included with a software package at the time of purchase.

FILE: A file is an entity of data. Files can be program files, which contain instructions that allow the computer to perform various tasks under the control of the user, or data files, that contain information only. The file must have a unique name within its own directory.

FOLDER: synonymous with directory, the term folder is more common in systems such as the Macintosh or Windows products which have a graphical user interface and provide a graphical file browser in which directories are traditionally depicted as folders.

LAN: means Local Area Network or a system served by one or more file servers.

LICENSE AGREEMENT: means a contract between the software publisher and the intended user.

LOG-IN NAME: is the unique account name assigned a used to access a computer system. Also called user ID or username. A log-in name may be derived from the first seven letters of the employee's last name and the first letter of his/her first name. (i.e., User: George Brown, Log-in Name: gbrowne.)

LOG-IN PASSWORD: a unique code or word linked to the log-in name that is used by an individual employee to gain access to a computer resource.

MOBILE DATA: means a laptop computer used as a mobile workstation for field access to our network of information sources (i.e., CAD, IMC, COLLECT, CAPTAIN, BLUELINK, etc.) The term is synonymous with the term workstation, as used throughout this policy.

NETWORK OPERATION: Logging onto or using a workstation, application, or program linked to or installed on a file server.

POWER-ON PASSWORD: a password assigned to a computer that prevents other users from starting the system.

SYSTEM ADMINISTRATOR: Person(s) responsible for the operation and maintenance of all software, workstations, file servers, and peripheral equipment. May also be referred to as the Information Technology Technician.

USER: means employee, any natural person, corporation, trust, incorporated or unincorporated association and any other legal entity or governmental entity, including any state or municipal entity or public official.

WORK PRODUCT: any electronic document, spreadsheet, digital image, program or other file that is created or produced on a town resource.

WORKSTATION: All computer-related hardware including, but not limited to, processor, keyboard, monitor, printer, mouse, trackballs, scanners, digital imaging devices, modems, UPS devices, surge protectors, cables, connectors, adapters, telephones, and any other device attached to any component.

V. System Administration

The Information Technology Technicians shall have administrative responsibility for all town computer hardware, software and data resources. The terms Information Technology Technician and Information Technology Department are used interchangeably throughout this document.

VI. Use of Computers and Computerized Information

The Town of East Windsor prohibits the dissemination of any town owned or shared information, in any form, contained in or accessed through the town's computers, to any other person, except one who is officially entitled to receive such information, without having approval of either the First Selectman, specific departmental head or their designees or under due process of law (See section entitled Requests For Electronic Data).

Accessing or attempting to access systems, files or documents belonging to the town or a third party, when not related to the performance of your job assignment is prohibited. For example, attempting to access or view anything in the town's information network for the purpose of satisfying curiosity is clearly inappropriate.

Employees shall not use any town computers or software for personal reasons.

Employees learning of or suspecting any misuse of the town's computer resources, including its hardware, software, related documentation, mobile data, or Requests for Electronic Data should alert the Director of Technology or the First Selectman.

All requests for electronic data made pursuant to the F.O.I.A., subpoena, or other court order shall first be referred to the First Selectman.

If the information request requires the statistical compilation, preservation or duplication of electronic records, the request shall thereafter be forwarded to the Information Technology Department for processing. All documents, prior to release, shall bear the town's validation stamp, the transaction date, and the processing employee's initials.

VII. Improper Use of Computer Systems & Information

Improper use of computerized information includes the following non-exhaustive list of activities:

1. Obtaining information or using any town resource in violation of law, regulation, policy, procedure, or other rule.
2. Release or use of records for personal or financial gain, or to benefit or cause injury to a third party.
3. Use of any town resource for access to or distribution of indecent or obscene material or child pornography.
4. Harassing other users, or tampering with any computing systems, and/or damaging or altering the software components of same.
5. Use of town resources for fundraising, commercial or political purposes, benevolent association activities, or any other activities not specifically related to a business necessity of the town.
6. Any activity which adversely affects the availability, confidentiality, or integrity of any system resource and/or related data.
7. Engaging in acts that are deliberately wasteful of computing resources or which unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, broadcasting unsolicited mailings or other messages unrelated to the business necessity of the town, creating unnecessary output or printing, or creating unnecessary network traffic.
8. Data accessed through third party resources, including, but not limited to: NCIC, COLLECT, SPIN, NESPIN, and LEO, are regulated by a myriad of federal and state law and administrative regulations and shall be exclusively restricted to use by duly authorized employees and/or criminal justice agencies in the performance of their official duties. Employees shall adhere to all third-party security agreements governing the authorized access and use of the relevant databases.
9. All electronic traffic (email, internet and so on) is subject to tracking and record archiving per user.

VIII. Computer Software

Illegal or unauthorized use of software may have severe consequences, including legal action for an injunction barring further use of the software and actions for monetary damages and penalties.

In most cases, the town does not own all rights to software developed by a third party. Instead, the town's rights are governed exclusively by a license agreement. Unless expressly authorized by the license agreement, the town does not have the right to reproduce either the software or its related documentation. It is the policy of town to respect all computer software copyrights and to adhere to the terms of all software licenses to which all departments within the town and its employees, are a party. The town prohibits the illegal duplication or use of computer software, whether developed by its own employees or by third parties.

Each employee using original issue, commercial copyrighted software shall do so only in accordance with any applicable license agreement and departmental policy. Town proprietary software is to be used only to conduct the town's business and is not to be copied for personal use or transferred to third parties for use without administrative authorization and without execution of

appropriate licensing documentation. Upon termination of employment, the employees shall return to the First Selectman or departmental supervisor all department and third-party software in their possession. Employees learning of any misuse of software or related documentation within should contact the Information Technology Department or the First Selectman's office.

IX. No Privacy Expectation for the Town's Computer Files

Employees have no expectation of privacy beyond those accorded non-employees in the files stored on the town computers, networks, tapes, or removable media. These files may be accessed by the town's technical or supervisory personnel without notice.

The assignment or use of a system password implies no ownership rights or any expectation of privacy on any town computer resource.

Supervisors needing to access any password protected or encrypted files **of an absent employee in order to facilitate the business needs of the town shall contact the Information Technology Department. An employee shall provide all keys or passwords to files that have been encrypted or password protected upon request of either the Information Technology Department, First Selectman or the Departmental Supervisor.**

X. Use and Care of Equipment

Employees are reminded that the Town's workstations are of vital importance to the productivity of the town. These costly and environmentally sensitive electrical devices require proper use and care. Therefore, employees shall adhere to the following guidelines to ensure the equipment is handled with due care:

- Keep feet and legs off the equipment.
- Do not expose any equipment or components to liquid, dust, heat, shock, or magnetic influence, nor permit the accumulation of materials likely to restrict the systems ventilation.
- Do not unplug workstations from surge protectors or UPS devices.
- Do not unplug, reconfigure, or move computer components from their original location without prior approval from the Information Technology Department.
- Do not disassemble computer components or workstations unless approved by the Information Technology Department. This section does not apply to personnel specifically trained to replace disposable items such as printer paper, ribbons, and ink or toner cartridges.
- Notify your supervisor of damage or equipment malfunctions involving any workstation.
- When operating a vehicle equipped with a mobile computer, the safe operation of the vehicle is an employee's primary responsibility. Use of the computer is always of secondary importance, and the employee should consider the need to safely stop the vehicle before using the computer if the use is going to divert the employee's attention from the safe operation of the vehicle.
- The Information Technology Department should be immediately notified if a mobile workstation has been stolen, or unauthorized access was attempted or gained, in order to implement procedures to safeguard the integrity of our networked resources.

XI. Operational Guidelines

A. Generally

- Employees shall not delete, erase, alter or format drives, directories, disks, files or folders without authority to do so from the Information Technology Department.
- Employees shall not copy or otherwise create an image of any program without authorization of the Information Technology Department.
- Employees shall not copy or otherwise create an image of any file not specific to the performance of their job requirements without authorization of the Information Technology Department.
- Only software authorized by the Director of Technology or the First Selectman will be installed, loaded, or otherwise used on a town workstation.
- Software authorized for use must be scanned for virus contamination and installed by the Information Technology Department.
- Employees will not configure, modify, partition, or alter any predefined hardware or software configuration setting, including, but not limited to, the CMOS/MOS setting, CONFIG.SYS or AUTOEXEC.BAT files, registry or hard disk, located in any town computer resource.
- Employees experiencing difficulty in operating a workstation will not turn off or unplug the computer without first contacting the Information Technology Department.
- No computer shall be equipped with or attached to an external communication device designed for remote operation or connection (i.e., a modem) without prior written authorization from the First Selectman.
- In order to prevent unauthorized access to the town's computer system from an outside source, any desktop computers equipped with network access and an external communication device (i.e., a modem) shall not be left in an operational mode (i.e., host mode).
- The operation of any system resource while utilizing a password or access privilege other than your own is prohibited.
- In the interest of security, employees shall not leave desktop workstations unattended without logging/signing off.
- Employees discovering any security violations or system vulnerabilities shall notify the Information Technology Department so that corrective action can be taken.
- It is the responsibility of employees assigned to vehicles equipped with computers to safeguard such devices. Vehicles so equipped will be locked at all times when the vehicle is unoccupied.

B. Requests for installation of software or hardware enhancements.

1. When a desired modification is requested, submit interoffice correspondence to the Information Technology Department. Correspondence shall include the following:

    - The name and type of enhancement the employee is requesting.
    - The business necessity for the proposed modification.
    - How the modification will enhance the work performance of the Department/Unit and/or employee.
    - What computer(s) will be affected by the modification.
    - The proposed storage location of any applicable User’s Manual.

2. If approval is granted, the following shall be adhered to:

- The legal copy of any software must be owned by the Town.
- The original distribution disks and the User's Manual must be presented as proof of ownership.
- The User's Manual must remain in close proximity to the computer to allow all authorized users to utilize the software.
- The original software distribution disks shall be retained by the Information Technology Department.
- All related installation and configuration of approved software shall be performed by the Information Technology Department.

C. System monitoring

1. The Information Technology Department shall periodically monitor and audit the entire system. If any unauthorized software, hardware, or other system modification or policy violation is discovered, the Information Technology Department shall:
   - Document and report the discovery by sending interoffice correspondence to the First Selectman.
   - Assist in any subsequent system review and/or investigation.
   - Restore the integrity of the system configuration and remove any software, hardware, or password access as directed.

XII. Importing/Downloading Information and Software.

A. Employees shall not download, or install on any computer, any file including sound or video files, files attached to e-mail messages, software, or any other materials without taking the following steps to preclude infection by computer viruses.

1. All electronic resource material shall be scanned for viruses prior to being introduced into any Town computer system.

B. Employees shall observe the copyright and licensing restrictions of all software applications, documents, images and sound or video files, and shall not copy such items from internal or external sources unless legally authorized.

1. Any software for which proof of licensing (original disks, original manuals and/or license) cannot be provided is subject to removal.

2. Privately owned software may not be loaded on any of the town computer resources.

XIII. Electronic Messaging

The e-mail and messaging systems, including but not limited to, GroupWise, Instant Messenger and Internet communications on any of the town's computers are an extension of the work place, intended to enhance communication and productivity. The following provisions are designed to ensure that this business tool is used in a professional and responsible manner. These systems are

wholly owned and solely operated by the town and shall only be used by employees for the purpose of conducting town business. The use of a password shall not imply any right of personal privacy in the contents of any e-mail communications.

Transmission of electronic messages and information on communications media provided for members of this town shall be treated with the same degree of propriety, professionalism, and confidentiality as official written correspondence. Electronic messages and documents are subject to the same requirements as information communicated in other written forms and formats. E-mail messages are considered public records. Therefore, they are legally discoverable and subject to record retention policies.

The town reserves the right to periodically audit, monitor, retrieve, review or disclose e-mail and messages sent and received at any time, with or without prior notice, to employees. By using the electronic mail and messaging systems, you expressly consent to the town's monitoring, auditing, reviewing, retrieving, disclosing and otherwise tracking the use and content of e-mail and messages. Supervisors needing to access the e-mail of an absent employee in order to facilitate the business needs of the town shall contact the Information Technology Department.

Employees shall not misrepresent themselves when sending an electronic message. Employees shall not communicate, display or forward any statement, comment, epithet, image, cartoon, software, etc. which could be construed as harassment or offensive to others based on race, religion, age, national origin, sex, sexual orientation, disability, political beliefs or other classifications protected by state and federal law. Transmitting materials (other than that required for town business) that involve the use of obscene language, images, jokes, sexually explicit materials, or messages that disparage or otherwise embarrass, annoy, harass or offend any person, group, or classification of individuals is prohibited.

Employees shall not transmit any image or text which may be protected by copyright, trademark or patent without prior permission.

XIV. Passwords

Your password is your first line of defense against unauthorized use of your assigned computer resources. If someone guesses or otherwise acquires your password, that individual can impersonate you. This embarrassing situation will compromise the integrity of the town's computer system resources. Employees shall keep their passwords secure at all times.

The Information Technology Department shall assign a network log-in name and initial network log-in password to all authorized employees. All employees will be required to change their network password upon their first log in.

Some town software applications will require the use of an additional application name and password. Where the security protocols for these specific applications differ from this policy, such differences will be provided with the instructions governing the use of such applications. Application passwords may or may not be assigned depending upon the application and the work assignment of each employee.

Employees shall adhere to the following requirements for the design and use of passwords for all town computers:

1. Your password should contain characters from at least 2 of the following 4 classes and preferably 3 of the 4 classes:

1. English Upper Case Letters	A, B, C,…Z
2. English Lower Case Letters	a, b, c,…z
3. Westernized Arabic Numerals	0, 1, 2, …9
4. Non-alphanumeric ("special characters")	For example, punctuation, symbols. ({}[],.<>;:'"/|\`~!@#$%^ &*()_-+=)

2. At a minimum your network and password must be at least 8 characters long. For stronger security, choose longer passwords with characters from all four classes.

3. Your password shall not contain your e-mail name or any part of your full name. It shall not include birth dates, social security numbers or any part thereof, maiden names, pet names or marker plate numbers. They are too easy to guess.

4. New passwords cannot be the same as any previous password.

5. Your password shall not be a "common" word (for example, it should not contain words from any language, because numerous password-cracking programs exist that can run through millions of possible word combinations in seconds.

6. Do not use repetitive or patterned characters; for example, AAAAAAAA or ABABABAB.

To come up with a strong password as outlined above, and one that is easy to remember, start by thinking of a short phrase that you can easily recall and is meaningless to others. Your phrase might be: "I began working at #16 years of age!" By combining selected letters and characters you form an incomprehensible password: "Ibwa#16yoa!". You can remember the phrase but nobody else is likely to guess it.

User-ID codes and passwords shall not be attached to terminals, desktops, or located where accessible to any other person.

No employee shall access or allow others to access any file or database unless that person has both a need and a lawful right to such information. Additionally, personal identification and access codes shall not be revealed to any unauthorized person.

If the employee suspects that the security of his or her password has been breached, the employee shall change the password immediately and promptly notify the Information Technology Department so that action may be taken to safeguard the integrity of the town's resources.

Access to the town's computer resources is commensurate with an employee's level of responsibility within the town. Therefore, access through a user profile is subject to modification concurrent with an employee's change in work responsibility.

XV. Personal Conduct and Responsibility

I understand that any violation of applicable law by me could result in my department being prohibited from having further access to computerized information; that I could be forbidden further access to any terminal and its information; that I could become the subject of an official investigation which could lead to my arrest and conviction for violation of State and Federal laws and regulations designed to protect the confidentiality of computerized information; that I can be subjected to a town investigation and disciplined, up to and including termination, if found to have violated these information protection laws, this policy or other applicable town rules and regulations.

XVI. Agreement on the Use of Town Computer Resources

The acknowledgment agreement referred to in Section I of this document follows on the next page and is to be executed by the employee and returned to the First Selectman's office.

Effective March 30, 2009

Town of East Windsor

Agreement on the Use of Town Computer Resources

By signing below, I hereby acknowledge that I have received and read a copy of the town's policy entitled, "**TOWN OF EAST WINDSOR COMPUTER/NETWORK ACCEPTABLE USE POLICY**," and I agree to adhere to the contents of this policy. I have been afforded an opportunity to discuss and resolve any questions relative to the contents of this policy and will be provided instruction on the requirements set forth in this policy by the Information Technology Department.

Read, understood and acknowledged by: _____
Signature of Employee

_____
Print Name

_____
Date

Witnessed by: _____
Signature of Witness