TOWN OF BEEKMAN

Computer Use Policy

Adopted July 2, 2014

Table of Contents

INTRODUCTION

This document sets forth the rules of conduct and guidelines for appropriate and efficient use of the various computer and other information systems employed by the Town of Beekman. The policies in this document are in conformance with New York State Cyber Security Policy P03-003 revised February 2010 and New York State General Business Law 899-aa.

The following rules and guidelines apply to, but are not limited to, personal computers, data storage and printing devices, electronic mail, telephones, facsimile machines, voice mail, toll free communications and internet access. All of these systems are provided to authorized individuals for the purpose of conducting official Town of Beekman business. These systems allow users to access and process information and communicate with other individuals worldwide in the performance of their job. These systems must be used in a secure and efficient manner. It is the responsibility of each user to assist the Beekman Town Board in complying with this policy.

In order to enforce policy statements regarding use of these systems, **the Town Board reserves the right to monitor your activity on its computer and telecommunication systems.** Monitoring may be preformed on both a routine and random basis for the purpose of assuring quality performance and appropriate use of these systems. In addition, the office may from time to time need to access messages of the employee for backup, maintenance, emergency or other administrative purposes. **Users, therefore, should not have any expectation of personal privacy with respect to any message sent, received or stored on any of these systems.**

POLICY

Business Use

These Systems must only be used for conducting Town business or for purposes authorized by the Town. **Use is subject to audit at any time by the Town.** Personal use of these business systems may be approved by the Town Board, but only if such use is clearly insignificant, does not interfere or compete with Town business, and does not involve any incremental cost to the Town. These systems and the data that reside on them are the property of the Town of Beekman and must be protected from loss, modification or destruction. **No employee should have any expectation of privacy regarding use of the Town's Information Systems**.

E-Mail

Users should be aware that the Town may review stored e-mail messages, so users should have no expectation of privacy when using these systems. E-mail messages are defined as any written or recorded messages delivered over or through the Town personal computers, wide and local area networks, and any Town supplied portable communication devices. The Town recognizes that personal communication among co-workers is a natural and pleasant outgrowth of working together and that personal communications with family members or other external associates occasionally occurs during working hours. However, users should make every effort to limit personal communications using Town e-mail systems. The Town has provided computers and telecommunications capabilities, including e-mail, to be used for the purposes of conducting Town related business. As a result, **All e-mail messages are the property of the Town.** The information may be subject to Freedom of Information Law (FOIL) requests under the Public Officer's Law and discovery demands under State, Federal and Local Law regulations. E-mail users are responsible for ensuring that individuals with whom they communicate also adhere to the Town's policy regarding prohibited activities. Users should observe common rules of etiquette and not include anything in an E-mail message that they would not want to say in the presence of their superior, in a courtroom, Town residents or to the addressee.

All email accounts used for conducting Town business must be authorized by the Supervisor and Supervisor and Comptroller. At no time should an employee or official create an email account on behalf of the Town of Beekman outside of the TownofBeekman domain. Email accounts such as Gmail, Outlook, Yahoo or AOL cannot be used for conducting Town business.

Internet e-mail poses the most significant threat to the Town in terms of viruses, worms, and other external threats. Users are expected to use caution before opening E-mail attachments from unfamiliar sources.

Junk E-mail (SPAM) is also becoming a significant drain on network resources, users should give careful consideration before giving out their office e-mail address to commercial entities. Many internet businesses sell their address lists to bulk spammers.

Software Licenses

Trademarks, copyrights and patents must be respected. Individuals must not retrieve, reproduce or post software or other intellectual property that is protected by trademark, copyright or patent law unless permission is obtained. Permission must be explicitly provided and documented by the copyright or patent holder.

It is a violation of Town policy to attach executable software files to E-mail messages where the Town does not hold the copyright, and therefore does not have the legal right to transfer ownership or license to the software. Users who receive E-mail messages with attached executable software files must ensure that the Town has a valid license for use of the software. Users who receive software in this manner should coordinate with the Town Supervisor and Comptroller to ensure that the software is compatible and acquired legally. No duplication or copying of licensed software is permitted, except as explicitly allowed in the license terms and conditions.

Prohibitions

When using these systems, you should not misrepresent yourself, (i.e. masquerade as someone else on a system). You cannot monitor network traffic (i.e. use a "sniffer" or similar device) without first obtaining explicit approval from the Town Supervisor and Comptroller.

Connecting a bridge, router, gateway or modem, or any wireless device to Town computers without first obtaining permission is not allowed. **Under no circumstances should a workstation attached to a network be equipped with a modem containing dial-in capability.** The Town has installed a variety of firewalls, proxies, internet screening programs, and other security screening systems to assure the safety and security on Town computers and networks. Any employee who attempts to disable, defeat, or circumvent any Town security facility could be subject to disciplinary proceedings, termination of employment and possible prosecution.

Additionally, these systems may not be used for illegal purposes or purposes contrary to the Town's ethics or policies documents. Harassing, intimidating, or defaming another individual or organization by issuing offensive or disparaging statements or language based upon race, culture, sex, age, disability, religion or any other personal attribute is not permitted. The disruption of users, services, or equipment at the Town's locations or any other site accessible from the Town's locations is not allowed. You should not attempt to repair hardware or software related issues. Unauthorized personnel are prohibited from contacting outside vendors or consultants directly regarding Town owned computer equipment.

Internet access for personal use is allowed to the extent it is clearly insignificant as compared to your business use. Users may never solicit other Town employees or provide information about, or lists of, Town employees to others and must comply with the security and use guidelines described within this document.

Additionally, when using electronic mail to communicate with people on the Internet, do not send mail so that it appears to have come from someone else, do not send unsolicited advertising via mail and do not send or reply to chain letters. Automatically forwarding Town Internet mail to an Internet site or using auto-reply functions to respond to your Internet mail is not permitted.
If you use auto-reply functions for your normal Town Internet mail when you are away, be sure to select the option that excludes sending the notices to Internet users.
Do not use personal e-mail addresses to send internal Town e-mail to another Town employee. Always use the employee's office e-mail address.

The following are other examples of conduct involving the use of our computer system which are prohibited:

- Sending an anonymous e-mail message.
- Sending or posting a discriminatory, harassing, or threatening message or image.
- Sending or posting a message that defames or slanders an individual or the Town.
- Sending or posting a message that disparages an individual's or company's products or services.
- Sending or posting a message or material that could damage the Town's image or reputation.
- Sending or posting a chain letter, solicitation, or advertisement not related to business purposes or activities.
- Sending or posting confidential material, trade secrets, or proprietary information outside of the Town.
- Using the system to engage in any illegal activity.
- Using the system for personal gain.
- Using the system for unauthorized transactions that may incur a cost to the Town.
- Stealing, using, or disclosing someone else's code or password without authorization.
- Attempting to break into the computer system of another individual or company.
- Copying or downloading software and electronic files without permission.
- Violating copyright law.
- Failing to observe licensing agreements.
- Intentionally or carelessly transmitting a virus or introducing it into our system or any other system.
- Participating in the viewing or exchange of pornography or obscene materials.
- Passing off a personal view as representing that of the Town.
- Jeopardizing the security of the computer system.
- Failing or refusing to cooperate with a Town investigation involving the computer system.

Elected and Appointed Officials

All Board members including Planning and Zoning conducting Town business from computers outside the Town's network must adhere to The Town's "Computer Use Policy".

Any communication such as e-mail correspondence that pertains to Town business is the property of the Town Of Beekman regardless of its origination and is subject to FOIL (see section under E-Mail for definition)**. Elected and Appointed officials, therefore, should not have any expectation of personal privacy with respect to any message sent, received or stored on any computer when conducting official Town business**.

The Town of Beekman routinely videotapes Town Board meetings for air on Vimeo Channel 111324 for webcast on the Town's official website: www.TownofBeekman.com. The Town reserves the right to videotape any public meeting held for the purposes of conducting Town business. **Elected and Appointed officials, therefore, should expect that there will be both audio and video recordings of them during public meetings.**

SECURITY

Protecting Computer Workstations

Every employee is responsible to help reduce the possibility of theft of Town computers and the information they contain. **The operation of the computer will be subject to audit by the Town.**

The use of memory sticks, thumb drives, flash memory cards such as XD, SD, Micro, Mini, CF, MS, cards etc., cameras, portable music players and Personal Digital Assistants are expressly prohibited on Town equipment unless authorized by the Town Board. Excluded are Town issued smart devices which are required to have anti-virus protection on them. All remaining removable media such as external hard drives, CDs or DVDs and CD/DVD reader/writer items must be scanned with a virus scanner prior to use.

When you leave your work area at the end of the day, if you work in an office that can be locked and where local health and safety regulations allow, you should lock the office. If you use a laptop computer, lock it in a desk or filing cabinet or other secure place. If logged onto the Internet, it is important that you log out before leaving your workstation for any extended period of time.

All workstations are to be logged off by the user at the end of the day and shut down at the end of day on Fridays.

When traveling, keep portable computers in your possession. Do not leave them exposed in cars or hotel rooms, with hotel personnel and do not check them into airport baggage.
When traveling by car, lock the computer in the car trunk when you begin your travel and upon reaching your destination, if you must leave the computer in the car, leave it locked in the car trunk. Always make certain that password security features are enabled and that passwords remain secure and confidential.

When staying at a hotel, if you must leave the computer in the hotel, lock it in the hotel safe, if one is available. If a safe is not available, store the computer out of open view in your hotel room. Do not connect a laptop to a non-Town network unless you have prior approval from the Supervisor and Comptroller.

Protecting Classified Information

The primary requirement for protecting the Town's confidential information is that access to it may only be given to people who have a need to know the information. Internet servers/websites must never allow unrestricted access (for example, world readable, public, etc) to the office systems.

Transmission of confidential information via the Internet e-mail systems is to be prohibited without prior approval of the Town Supervisor and Comptroller. When appropriate, encryption technology should be employed to ensure privacy of confidential information. A typical electronic mail message traversing the Internet passes through many computers along the way.

An Internet message may also cross several servers or Post Office on its way to the recipient. Although somewhat unlikely, a message can be intercepted by a hacker or by any number of individuals who administer external systems. Also, if your message is not addressed correctly, it may end up in the wrong place either internally or on the Internet and may be accessed by someone other than the intended recipient. In general, think before you send an e-mail. It is not private and once sent, it cannot be recalled.

Confidential information accessed through or transmitted across the Internet must be protected by encryption technology (for example date and/or session encryption) approved by the Town Supervisor and Comptroller.

If you receive another company's classified data from the Internet, you must comply with that company's instructions for protecting the data. Employees and Elected & Appointed officials who use Town email on personal Blackberry's and smart phones should have antivirus protection on these phones to protect Town confidential email.

PCI COMPLIANCE

Protecting Personal Information

The Town of Beekman is committed to protecting the privacy and personal information of the public. All department and branches of government operating within the offices of the Town must comply with this policy.

All card processing activities and related technologies must comply with the Payment Card Industry Data Security Standard (PCI-DSS) in its entirety. No activity may be conducted nor any technology employed that might obstruct compliance with any portion of the PCI-DSS.

Applicability and Availability

This policy applies to all employees: full-time and part-time, temporary and personnel, contractors and consultants working on behalf of the Town of Beekman.

Best Practices

When using credit card appliances:

Personnel processing credit card transactions must comply with rules, regulations and training set forth by the State agency with jurisdiction over their department.

Secure credit card device at all times and do not leave unattended.

Keep paper copies of transactions and photocopies away from open public areas.

All employees must adhere to additional rules set forth in any additional Town Policies.

INTERNET

Access to the Internet

The Internet is a rapidly growing and important resource for the Town. Efficient use of the Internet can provide an advantage in the form of cost savings, improved service, and new ways of doing business, information gathering and improved external communications.

This document describes the basic Internet usage and security measures all employees are obligated to follow.

Internet access includes, but is not limited to: viewing websites, sending and receiving
e-mail, transmitting or receiving files and running Internet applications.

As we use the Internet, it is important to remember that the Internet is used by millions of people worldwide and not all Internet users have the Town's best interests in mind. You should presume that any unprotected information sent across the Internet will be read by a number of unknown people.

You must not allow ANONYMOUS FTP, TFTP, PIF or other unauthenticated access to program or data files on your computer.

Access to the Internet from any Town computer must be through a firewall. Individuals using office systems are not permitted to access the Internet via direct dial-up connection (i.e. CompuServe, America On-Line or any other third party Internet service provider). Exceptions to this policy must be approved by the Supervisor and Comptroller and Town Board. Third party dial-up access will be permitted only where there is a documented logistical need, legal requirement or other exceptional job responsibility.

Connecting to the Internet

Connecting office systems to the Internet can present a very serious risk to the Town. The technology involved in establishing a new Internet connection, a new Internet gateway/firewall, or a new Internet server is relatively simple. However, the technical and administrative controls necessary to protect that service against highly skilled Internet hackers can be very complicated and labor intensive.

It is possible to expose all Town systems and data on it, without even knowing you are doing so.

Privacy

Internet usage and web browsing habits can and will be monitored. No expectation of privacy exists when using the Town's internet connection.

Harmful Code/Viruses

Be aware that there are potential dangers in accepting programs or viewing data from unknown sources on the Internet. Town employees are not to send or forward e-mail notice concerning virus or harmful code warnings to other employees.
If you receive an e-mail notice about a supposed virus or harmful code threat, you should advise the Town Supervisor and Comptroller immediately.

Other forms of harmful code can act similar to a computer virus, but are not transmitted by copying and executing infected programs. These newer forms of attack are activated by simply viewing a web site that contains maliciously programmed applets or JavaScript.

Web sites established by individuals (other than companies), and web sites established by organizations with questionable ethics, are prime candidates for hosting harmful code. You should avoid these sites whenever possible.

To help guard against harmful code, before visiting an internet website the security control options in your web browser must be set to prohibit execution of applets or JavaScript and the receipt of "cookies".

Town employees and appointed officials holding an Internet e-mail address may be recipients of unsolicited non-business e-mail (sometimes referred to as spam or junk). This situation is similar to receiving unsolicited telephone calls or unsolicited postal mail.

The easiest and generally most effective response to unsolicited e-mail is to ignore the mailing. In specific cases where individuals or organizations on the Internet demonstrate themselves to be a continuous source of unwanted or unsolicited e-mail, the Town may choose to apply technical control measures to prevent the receipt of further mailings from those individuals or organizations.

Conduct

When accessing the Internet from a Town addresses designation you must adhere to the security and usage guidelines in this document. Use only services you have authorization to access and do not try to get into open Internet systems or server ports without prior authorization. Do not run security testing tools/programs against any Internet system or server without explicit authorization from the system/server owner. Always represent yourself as yourself, never someone else.

Only those employees or officials who are duly authorized to speak to the media, to analysts, or in public gatherings on behalf of the Town may speak/write in the name of the Town to any newsgroups or chat rooms. Please remember that the laws of slander and libel apply to Internet communications. Do not place or access any material on the Internet that would be considered vulgar, offensive or disrespectful to others.

Additionally, Town employees, Elected Officials and Appointees must seek assistance and approval from the Town Supervisor and Supervisor and Comptroller before incorporating anything downloaded from the Internet into a Town computer. Even the tiniest programs downloaded from the Internet can contain viruses or worms harmful to system integrity and security (i.e. screen savers and weather alerts).

Inappropriate Internet Web Sites and Technology

Numerous Internet web sites contain distribute material that is objectionable in the workplace. While it is impossible to list every possible web site or form of objectionable material, some clear examples include sites that contain sexually explicit images and related material, advocate illegal activity or intolerance for others.

Town employees are not to access such web sites, or distribute or obtain similar material through the Internet. **Compliance with this policy is a condition of employment**. Social media and shopping sites will be blocked for employees who do not require their access as part of their duties. The Town does not maintain a complete list of inappropriate web sites. Town employees should not therefore presume that the Town approves access to all web sites not blocked by Town control measures.

If Town employees' access to specific web sites containing inappropriate material becomes a source of embarrassment to the Town due to the news media or trade press reports, the Town may choose to apply technical control measures to prevent further access to those sites.

Instant messaging programs such as Yahoo Messenger or AIM should not be downloaded and installed on office computers. Such programs have been exploited to allow unauthorized access through network security devices.

The use of streaming media applications, such as Windows Media Player, and Real Audio Player should be kept to a minimum. Streaming video and audio applications consume significant amounts of network bandwidth. Several employees using such applications at the same time will severely diminish Internet communication speeds for the entire office. Streaming of Board Meetings from Town computers is discouraged during normal business hours except for those employees responsible for generating meeting minutes. The Town of Beekman reserves the right to block access to streaming meetings.

Peer to Peer file swapping services such as Napster, Kazaa, LimeWire, Morpheus, etc., significantly impact network security. Use of these applications is expressly prohibited at all times.

Social Networking sites such as Facebook, Tumblr, Twitter, Linkedin, etc. are unauthorized sites within the Town of Beekman network and may be blocked.

ENFORCEMENT

All users of the Town of Beekman's information systems, computers and peripherals who are found to have violated any of these policies will be subject to disciplinary action up to and including (but not limited to) warnings, probation, suspension, discharge, dismissal, expulsion, and/or legal action. All users, when requested, are expected to cooperate with system administrators in any investigation of system abuse. Users are encouraged to report suspected abuse, especially any damage to or problems with their files. Failure to cooperate may be grounds for cancellation of access privileges, or other disciplinary actions.

Town employees and Elected & Appointed officials should be aware that e-mail on their Town account and files on Town computers may be subject to public disclosure under New York State Freedom of Information Law. Further, the Town of Beekman reserves the right to access employee e-mails and files on Town computers when needed for work-related purposes.

The Town of Beekman may temporarily suspend or block access to an account or computer prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of Town computing resources or to protect the Town of Beekman from liability. The Town may also refer suspected violations of applicable law to appropriate law enforcement agencies.

Incident Response

A designated representative from the Beekman Town Supervisor and Comptroller will receive, review and respond to any and all computer security incident reports and activity including any real or suspected adverse event in relation to the security of Town computer systems or computer networks as directed by the *Information and Security Breach Notification Policy.*

Employee Acknowledgement:

I have read and have been informed about the content, requirements, and expectations of the Town of Beekman Computer Use Policy. I have received a copy of the policy and agree to abide by the policy guidelines as a condition of my employment and my continuing employment at the Town of Beekman

I understand that if I have questions, at any time, regarding this policy, I will consult with the Town Supervisor.

Please read the Town of Beekman Computer Use Policy carefully to ensure that you understand the policy before signing this document.

Employee Signature: _____

Employee Printed Name: _____

Date: _____

Vendor and/or Consultant Acknowledgement:

I have read and have been informed about the content, requirements, and expectations of the Town of Beekman Computer Use Policy. I have received a copy of the policy and agree to abide by the policy guidelines as a condition of my business relationship with the Town.

I understand that if I have questions, at any time, regarding this policy, I will consult with the Supervisor and Comptroller, ISO or any Town Board member.

Please read the Town of Beekman Computer Use Policy carefully to ensure that you understand the policy before signing this document.

Business Name: _____

Authorized Representative: _____

Date: _____

This copy is for your files.

THIS PAGE LEFT INTENTIONALLY BLANK

Employee Acknowledgement:
I have read and have been informed about the content, requirements, and expectations of the Town of Beekman Computer Use Policy. I have received a copy of the policy and agree to abide by the policy guidelines as a condition of my employment and my continuing employment at the Town of Beekman

I understand that if I have questions, at any time, regarding this policy, I will consult with the Town Supervisor.

Please read the Town of Beekman Computer Use Policy carefully to ensure that you understand the policy before signing this document.

Employee Signature: _____

Employee Printed Name: _____

Date: _____

Vendor and/or Consultant Acknowledgement:

I have read and have been informed about the content, requirements, and expectations of the Town of Beekman Computer Use Policy. I have received a copy of the policy and agree to abide by the policy guidelines as a condition of my business relationship with the Town.

I understand that if I have questions, at any time, regarding this policy, I will consult with the Supervisor and Comptroller, ISO or any Town Board member.

Please read the Town of Beekman Computer Use Policy carefully to ensure that you understand the policy before signing this document.

Business Name: _____

Authorized Representative: _____

Date: _____
The completed and signed form should be returned to the Town Supervisor or Comptroller.