TOWN OF BEEKMAN, NEW YORK

Information Systems Usage & Security Policy

Adopted 08/25/2020
Revised 02/14/2023

Introduction and Policy Contact

This document sets forth the policies, regulations and procedures associated with use of the Information Technology Systems owned and operated by the Town of Beekman.

This policy applies to all elected officials, administrators, board members, employees, consultants and vendors of the Town who in any way access or use the Town's Information Systems.

The term Information Systems is used in this document to define all of the technical resources that provide the computing, communication, transmission, distribution and storage of information required and used by the Town of Beekman.

The term IT Manager is used in this document refers to the group of Information Technology Professionals currently charged with operating, supporting and maintaining the Town's Information Technology Systems.

The term User or Users is used in this document to refer to an individual or group of individuals that have been granted access to the Town's Information Technology Systems. Users can be elected officials, administration members, board members, employees, consultants or vendors.

This document has been authorized and approved by the Administration and Town Board and is to be adhered to by all employees, vendors, consultants, service providers and temporary workers (collectively referred to as Users) while accessing the Town's Information Systems from either Town premises or remote locations and systems.

This document and the Town's Information Systems policy is managed by Theresa Manzo, whose contact information is provided below. Please contact Theresa for all questions regarding this policy or any of its content.

This document will be revised from time to time as technology and / or the laws and labor agreements of the Town of Beekman change. It will be the responsibility of Theresa Manzo, working with the Town's Attorney's and IT Manager to revise the document and ensure all Users have the most current revision.

Information Systems Policy Contact

The Town of Beekman
Theresa Manzo
4 Main Street
Poughquag, NY 12570
Telephone - 845-724-5300
e-mail - accountclerk@townofbeekmanny.us

General System Usage

All users with a demonstrated need to access the Town's Information Systems in the regular performance of their job function will be granted access to the areas of the system required for their particular duties. All users provided with computer access are provided with a Town based e-mail account and access to the Internet.

Depending upon the department users are assigned to, Users may be provided with access to department specific software applications, MS Office applications and generic applications. Users are permitted to use these application as well as e-mail and Internet access as specifically relates to and associated with the performance of their job function at the Town. Please see the specific requirements related to e-mail and Internet usage in those named sections in this document.

System Access and Security

The Town's IT Manager is charged with maintaining security of the Town's Information Technology Systems. This includes user accounts, access to system resources and software applications, system backups, anti-virus updates and firewall control. The IT Manager is authorized to take whatever steps deemed necessary to protect the Town's systems and data from infiltration, exposure, damage and / or potential loss.

System security is the single most important factor relating to the use of the Town's IT systems. Each section of this document is, in some way, related to the security of the system. It is the responsibility of each system User to abide by and follow all rules and regulations related to IT system usage and if, at any point, is unsure of an action or actions that should be taken, they user should immediately contact the Town's IT Manager for advice and / or assistance.

In order to gain access to the Town's Information Systems, a user must first be authorized by either a department head or the Supervisor's Office. This process involves the authorizing person to complete and submit a **New User Form** to the Town's IT Manager. In completing this form, the Department Head provides the IT manager with the specific applications and areas of system access the new user is to be granted access to.

The Town's IT Manager will create the user account; assigning the user a login name, user rights and an e-mail address. E-mail addresses are standardized as the first letter of the user's first name along with the users last name @townofbeekmanny.us. Users will select their own password, which must be a minimum of 9 characters in length and contain upper and lower case letters, numbers and 1 special character.

Once assigned a login and password, users are responsible for protecting this information and may not reveal their login and password information to anyone, including other Town employees, associates or family members. Users may not allow any other person to access the Town's systems and/ or data using- their login and password and should not leave their computers on and unlocked when not at their desk. Users are responsible for any activity attributable to the use of their account whether by the user or any other person.

Users must never attempt to gain access to systems, data or information they are not authorized for. Users must never engage in activities that may cause interference with or disruption of the Town's IT systems. Attempts to do either are a violation of Town policy and may also violate applicable laws, potentially subjecting the user to civil and or criminal prosecution.

Vendor Access

Vendors, consultants and other such organizations doing business with the Town and having a demonstrated need to access the Town's Information Systems will be granted limited access coinciding with the vendor or consultant's need based on their particular relationship with the Town and as approved by the Town's IT Manager and/ or Administration. Under no circumstances will vendors be granted open or unrestricted access to Town's Information Systems.

Vendors of department specific software will be granted remote access to at least 1 workstation within each department their software application is installed for purposes of supporting their applications. Vendors requiring server console access to troubleshoot and resolve problems should be instructed to contact the Town's IT Manager for access to servers and assistance in resolving problems.

Department specific software vendors should be made aware that upgrades to their software must be planned and scheduled in advance with the Town's IT Manager. Those upgrades which are expected to require extended access to a server console and / or extensive loading of software to any of the servers will require the work be performed during slow usage periods or in off hours to minimize interruptions to Town operations.

Any User who knowingly violates remote access policies and I or system security will have their remote access privileges immediately and permanently revoked.

Safeguarding Sensitive and Personal Information

As previously stated, each User of the Town's Information Systems is granted access to applications and data based on their specific department membership and job function. Some of this information is "public", and as such has few restrictions on sharing and or distribution, while other information "sensitive" or "personal" including, but not limited to the personal information of employees and constituents and sensitive information relating to negotiations, human resources, investigations and/ or prosecutions. Sensitive and Personal information must be protected from exposure to unauthorized recipients at all times and may never be shared with or transmitted to anyone not having specific authorization and a need to access same,

It is the responsibility of each Department Head to insure all Users within their department are aware of the types of information they will be accessing. It is each User's responsibility to be personally aware of the types of information they are accessing and the requirements for same. If a User is unsure if the type of information they are handling is of a sensitive or personal nature, they should request clarification from their Department Head or a member of the Town Administration.

Some departments, such as Administrator, Finance, H/R, Police, Court and Clerk tend to handle more sensitive information than others; however users working in departments other than these should not assume they will not encounter sensitive or personal information in the performance of their duties.

Great care must be taken when copying, exporting, transmitting or transporting sensitive or personal information. Sensitive or Personal information should never be copied, exported or transmitted out of the Town's IT Systems without first encrypting the information to 256bit AES or higher encryption. If the User is unsure of the process of encrypting or decrypting of data, they should contact the Town's IT manager for assistance. Users should never transfer or transmit Sensitive or Personal information to any other party without first ensuring that the party is authorized to receive and possess the specific information being transferred or transmitted. If the User is unsure, they should seek guidance from their Department Head or the Town Administration.

Internet and Email

Internet Access and Usage

Internet access for this municipality is a business tool provided to Users at significant cost. The expectation is that Users will use the Internet for work related purposes only, i.e., to communicate with employees, constituents, vendors, consultants and other government agencies, to research relevant topics and obtain useful work related information except as outlined below. Users are required to conduct themselves honestly and approximately on the Internet, and respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others, just as you would in all other work related dealings on behalf of the Town.

All existing Town policies apply to your conduct on the Internet and with the use of Town e-mail systems, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of Town resources, sexual harassment, information and data security, and confidentiality.

Users may not import, download, copy or store copyrighted material without permission from the owner of the material or the Town's IT Manager. Doing so may violate application licensing agreements and or copyright laws. No software or other applications may be downloaded and/ or installed on any of the Town's IT Systems without specific authorization from the Town's IT Manager.

Users may never subscribe or post to non-work related Internet sites using the Town's systems or sign up for said sites using Town information and/ or e-mail addresses. Users may not create personal accounts of any nature using Town e-mail or contact information. This includes, but is not limited to sites, related to social networking, shopping, travel, sports, dating, file sharing or any other non-work-related subjects. Users may not order any non-work-related items or materials using Town e-mail or shipping address information.

Users may not harass, intimidate, or threaten others or engage in or visit sites promoting any illegal activity, which specifically include, but are not limited to; pornography, kidnapping, terrorism, espionage, theft or drugs using the Town's IT Systems. Any User who is subject to or observes such actions, is required to immediately report said actions to their Department Head or a member of the Town Administration. In addition to violating this policy, such behavior may also violate other Town policies, and/ or civil or criminal laws.

The Town's IT Systems may not be used for soliciting other employees for any reason, including but not limited to; any political or partisan activities, selling of products or merchandise or soliciting for fundraising. Users may never sign up to and/ or post on non-work-related sites on the Internet using the Town's systems and e-mail address. The Town reserves the right to access, review or otherwise monitor all Internet use.

Users may only use Video or Audio streaming technologies for specific work related activities such as training or research. These technologies can consume substantial amounts of bandwidth and impede the normal operation of the Town's Information Systems.

Users are advised that there is material on the Internet that is offensive and objectionable to most people. While the Town filters the vast majority of this material through its web filtering system, from time to time there may be some material that was not removed. Users must use good judgment and common sense to stay away from these sites. The Town disclaims any liability by any person who uses the Town's system and is offended upon discovering such sites.

Use of Social Media

The purpose of this section of the IT policy is to provide the framework for employee usage of Social Media both inside and outside of the workplace. Social Media in general refers to Internet based applications that allow for the creation and exchange of user generated content. Examples of Social Media include, but are not limited to: Facebook, Twitter, Instagram, Tumblr, Myspace, LinkedIn, Flicker, Imgur, YouTube, web blogs and web based wikis whereby users can add, modify or delete its content via a web browser.

Unless the use of Social Media is pertinent to Town business and authorized by a Department Head, employees are prohibited from using Social Media during working hours. This applies regardless of whether or not such usage occurs on Town-owned devices or a device personally owned by the employee.

The following uses of Social Media are prohibited by all Users at all times, regardless of the location from which the post is made or the device being used.

This list is meant to be illustrative, and not exhaustive.

- Disclosing confidential or proprietary information pertaining to matters of the Town that is not otherwise deemed accessible to the general public under the Freedom of Information Law (Public Officers Law Article 6, §§84-90).
- Matters which will imperil the public safety if disclosed.
- Promoting or endorsing any illegal activities.
- Threatening, promoting, or endorsing violence.
- Directing comments, or sharing images that are discriminatory or insensitive to any individual or group based on race, religion, gender, disability, sexual orientation, national origin, or any other characteristic protected by law.
- Knowingly making false or misleading statements about the Town, or its employees, services, or elected officials.
- Posting, uploading, or sharing images that have been taken while performing duties as an agent of the Town, or while wearing Town uniforms - the only except in to this rule is when it is directly pertinent to Town business and such posting, uploading, or sharing of images is authorized in advance by the appropriate Department Head.
- Representing that an opinion or statement is the policy or view of the Town or of any individual acting in their capacity as a Town employee or official or otherwise on behalf of the Town, when that is not the case.
- Posting anything in the name of the Town or in a manner that could reasonably be attributed to the Town without prior written authorization from the applicable Department Head.
- Using the name of the Town or a Town e-mail address in conjunction with a personal blog or Social Media account.

ACKNOWLEDGMENT OF RECEIPT

I, (print name) _____

hereby acknowledge that on this date I have received a copy of the Town's Information Systems usage policy adopted by the Beekman Town Board. I hereby acknowledge that I have read and understood the policy and procedures contained therein. I understand that if now or any time in the future I do not understand this policy or procedure, or I have a question about it, or I believe there has been a violation of the policy, that I must contact my immediate Supervisor or Department Head to resolve the situation. I agree to abide by this policy and specifically understand that violation of this policy may lead to discipline, up to and including termination.

Signature _____

Date _____