Beekman Information Systems Usage & Security Policy

December 4, 2017

Revision 2.00

Adopted By:

The Town Board

Table of Contents

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 the Town Supervisor Office, whose contact information is provided below. Please contact the Supervisor's office 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 the Town's Supervisor Office, 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
Peggy Matsuzawa
4 Main Street
Poughquag, NY 12570
Telephone - 845-724-5300
e-mail – secretary@townofbeekmanny.us

Operation, Maintenance and Management

Operation, maintenance and management of the Town's Information Technology Systems are outsourced to an IT Services vendor (hereinafter referred to as IT Manager) specializing in the operation and management of Municipal Information Systems. This vendor may change from time to time and if and when that occurs, the contact information provided on this page will be updated and a copy provided to all users.

The Town's IT Manager is currently Sullivan Data Management, based in Yorktown. Contact information for Sullivan Data is provided below. The Town's contract with Sullivan Data provides for all necessary services to support, manage, maintain and upgrade the Town's Information Systems. These services include the provision of help desk services to all users of the system.

Requests for support and assistance should be made by individual users directly to the IT Manager's support department using the contact information provided below. Support is available to all departments Monday – Friday 8:30AM – 5:00PM except national holidays.

Requests for upgrades and or expansions of the Town's IT system or any component of same should be made only by Department Heads to the Upgrade / Expansion contact listed below. Users and department heads should not enter into discussions with vendors regarding IT upgrades and / or additions without involving the Town's IT Manager. Users and department heads should also note that all IT expenditures will require the approval of the Town Comptroller and are subject to the Town's procurement policy.

Turn around time for upgrade / expansion work will vary based on the size and complexity of the work requested and the workload of the IT Manager's Project Team when the request is initially made. It is important when considering upgrades and / or additions, that you involve the IT Project Team when you first realize that you will need to upgrade existing or install new systems, and if possible, before you engage with any vendors.

Other Documents referenced in this policy, such as New User Forms or Remote Access Authorization Forms, are available by contacting the Town's IT Manager's Help Desk via the information provided below.

Support / Help Desk Contact Information
Sullivan Data Management
Support Team
1520B Front St.
Yorktown Heights, NY 10598
Telephone 914-962-8837
e-mail support@sullivandata.com

Upgrade / Expansion Contact Information
Sullivan Data Management
Project Team
1520B Front St.
Yorktown Heights, NY 10598
Telephone 914-962-1573
e-mail projectteam@sullivandata.com

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.

System Access and Security (cont.)
Department heads are responsible for notifying the Town's IT Manager in advance of employees leaving or changing positions and of impending terminations. Notification of termination should take place as soon as possible, but in no case not less than 24 hours in advance of employee notification.

Users are to understand that they should have no expectation of privacy in conjunction with the use of the Town's Information Systems, or with use, transmission, or storage of any information via these systems, especially with regard to Internet and E-mail activities.

The Town may, at its discretion, monitor, access, record or review any use of the Town's IT Systems; including but not limited to activity on the Internet and e-mail. In addition to stated monitoring, users should be aware that their activity on the Internet and e-mail may also become the subject of FOIL requests or legal subpoenas and as such, any and all of a User's activities while using the Town's Information Systems may be made public and if appropriate, subject to civil and or criminal prosecution.

Remote Access and Security
Remote access allows Users to access the Town's Information Systems from external locations. By default, each user is provided with remote access to their Town based e-mail account, which includes e-mail, address book and calendar information.

Users with a demonstrated need to remotely access other information contained in the Town's IT may request remote access to this information and / or applications. The request must be made through the Users Department Head or Supervisor or be specific in nature, stating the application or data access required and the reason the User requires remote access to the information. This request is made using the **Remote Access Authorization Form.**

Remote access to applications or data requires either a Town owned and managed portable computing device, such as a notebook or tablet, or a remote computer with a high speed Internet connection meeting certain specific criteria. Once remote access has been approved and if the User will not be using a Town owned device, the Users will need to fill out and submit the **Remote Device Information Form**.

Users who are granted Remote Access privileges who will be using Town owned and managed equipment are advised that they are solely responsible for the safeguarding of the equipment provided to them. This responsibility includes, but is not limited to protection from improper use, physical damage and theft.

Users are to never leave Town equipment unattended or in an unsecure location or unlocked vehicle. As previously stated, Users are responsible for safeguarding their login and password information and must never allow any other individual access to this information or to remotely access the Town's IT Systems. If a Town owned device is lost or stolen, the assigned User **must immediately** notify the Town's IT Manager so that the system access for that device can be disabled.

Users who are granted Remote Access privileges, and will be using personally owned devices and equipment are additionally advised that they are solely responsible for the operation and maintenance of their devices, equipment and Internet connections. The Town's IT Manager will assist in the initial setup of the connection and with connectivity issues between user devices and the Town's IT systems, but will not be responsible for troubleshooting or repairing user devices or other related computer or communications equipment.

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 / 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.

Networks and Computers

The Town's Information Systems are comprised of approximately 30 computers and other networked devices attached to Local Area Networks (LANs) in each physical building. These LANs connect the computers to the Town's servers, network printers and the Internet. The Town's servers are the repositories for all of the Town's information and data storage. Each server has been equipped with redundant power supplies, redundant drives and data backup systems to minimize the possibility of downtime and / or data loss.

Each User is responsible for ensuring the data and documents they create and manage on behalf of the Town are properly saved to one of the Town's servers, where it will be redundantly stored and backed up. Saving documents and data on a computers local (C:) drive is not safe and will potentially subject the data to loss without the possibility of recovery. If any User is unsure of where particular documents or data should be saved, they should contact the Town's IT Manager for assistance before attempting to do so.

Users are not permitted to install any software applications or hardware devices on any Town owned computer or computing device unless specifically directed to do so by the Town's IT Manager or one of the Town's department specific software vendors. Requests for hardware or software upgrades, modifications or additions should be directed to the Town's IT Manager by a department head using the contact information provided on page 3 of this document. Depending on the nature and size of the request, typical turnaround time for installation and / or upgrade work is approximately 30 days based on the IT Manager's workload at the time the request is made. Requests for installation / upgrade work allowing for less time should not be made.

Users may not use the Town's IT Systems for any personal use. This includes but is not limited to storing, printing or distributing documents, graphic files or e-mails.

Users may not export, copy, or otherwise remove from the Town's computer systems and / or facilities any data or software applications owned or licensed by the Town for any purpose, without specific written authorization by the Town's IT Manager.

Users may not copy, export, transmit or store Town data and / or information on storage devices and / or locations that are not owned or licensed by the Town. This restriction specifically applies to users personally owned devices such as smart phones and USB drives and personal storage accounts such as iCloud, OneDrive or DropBox. If users have a specific need to store data on these type devices or accounts to conduct the Town's business, they should contact the Town's IT Manager to provide same.

Users may not allow any unauthorized person to access their Town owned computer system, this specifically includes notebook and portable computers which are frequently taken and used off Town premises. Users should immediately notify the Town's IT Manager if they suspect another party is attempting to or has gained access to any Town owned computer, or if they suspect their computer may be infected with a virus or spyware.

Users provided with Town owned portable computers are responsible for safeguarding these systems from physical damage and /or theft. These units should be transported in a protective case and never left unattended in areas where others have access. If a portable computer is lost or stolen, the User assigned to the unit must immediately notify the Town's IT Manager so that the remote access to Town's IT Systems from this unit can be disabled.

Users should avoid exposing their Town owned computer system to environments that are hazardous to the operation of the system. These environments include, but are not limited to, all liquids, all food items, extreme heat or cold and high humidity.

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 appropriately 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.

E-mail Access and Usage

Each User of the Town's IT System is provided with a Town based e-mail account. Users are provided with storage capacity commensurate with their job function and expected use of the system. When accounts are within 10% of the storage capacity, users will receive a warning message to "clean up". If an e-mail account reaches the storage limit, the sending of new e-mail messages is disabled. Users with a demonstrated need for higher capacity storage limits should contact the Town's IT Manager. Requests showing a work related need will be granted.

The Town based e-mail account is to be used only for purposes directly related to the conduct of official business with the Town and shall not be used for nonpublic purposes including, but not limited to, the pursuit of personal activities, the mass distribution of unsolicited messages, the promotion of commercial ventures, or any political or religious causes.

Users may not create or forward nuisance e-mail, including jokes and chain letters. If Users receive a nuisance e-mail they should send a professionally worded response to the sender, requesting they be removed from the mailing list. If this action is not effective, the User should notify the Town's IT Manager so that additional steps can be taken.

Users of the Town's E-mail system should be keenly aware that they are, at all times, acting on behalf of the Town. All actions and communications should be conducted in the most professional manner possible. Users should be mindful that e-mail statements made to others may become binding commitments upon the Town.

Users should be aware that one of the most common ways of attacking and gaining access to IT systems is by use of "phishing attacks". Phishing is where Users receive an official looking e-mail requesting them to take an action such as clicking on a link or opening an attachment in the message. By clicking on the link or opening the attachment, a malware application is installed on the Users computer that is then used to bypass system security, and in many cases compromise system integrity or do damage to the data contained within.

As previously discussed, the Town's IT Systems contain a great deal of Sensitive and Personal information which could be compromised by a successful phishing attack. For this reason Users should be extremely careful when working with attachments or links within e-mails. Users should not click on any links nor open any attachments in messages from questionable or unknown senders. If the User is unsure if an e-mail is legitimate or not, they should immediately contact the Town's IT Manager before taking any actions.

Phishing attacks are now being used to infect systems with Cryptolocker type viruses. This is where the virus or malware encrypts every file that the infected User has access to. These viruses are especially damaging in network environments where they not only lock all files on the infected user's computer, but also lock every file that the infected user has access to on the organizations network. An infection of a User with high level access can affect thousands or 10's of thousands of files across multiple departments including important applications. An infection like this could expose the Town to embarrassment and / or liabilities.

To limit exposure from phishing attacks, Users may not access their personal e-mail accounts using Town owned computer systems. Users who need to access their personal / home e-mail during work hours may do so using their smart phones. Checking may take place during employee's breaks or lunch periods and should not interfere with the Town's business operations or with the user's ability to perform his or her job function.

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 exception 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.

Social Media (cont.)
An employee's Social Media usage must comply with Town policies pertaining to but not limited to Non-Discrimination and Harassment, Confidentiality, Violence in the Workplace, and Substance Abuse. Any harassment, bullying, discrimination, or retaliation that would not be permissible in the workplace is not permissible between co-workers online, even if it is done after hours, from home and on personal devices.

Notwithstanding the above, nothing in this policy is meant to imply any restriction or diminishment of an employee's right to appropriately engage in protected concerted activity under law.

Anyone with information as to a violation of this policy is to report said information to the appropriate Department Head. Once the Department Head is informed of the violation, a formal process, consistent with this Information Systems Usage Policy, Employee Handbook and/or applicable law, will begin.

Any employee who violates this policy will be subject to disciplinary action up to and including termination of employment.

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 _____