TOWN OF BEEKMAN, NEW YORK

SECURITY POLICY

Adopted 09/03/14

Table of Contents

Introduction **4**

Definitions **8**

Data Classification **13**

Policy Areas:

Acceptable Use 15

Account Management 17

Administrative and Special Access 18

Asset Management 19

Back Up 23

Court Information Resources 27

Email 27

Help Desk

Incident Management 29

Inter-Municipal Agreement 30

Internet 32

Intrusion Detection 33

Network Access 34

Network Configuration 36

Password 37

Physical Access 40

Portable Computing 42

Privacy 43

Public Access Workstation 41

Security Monitoring 44

Security Policy Standards 46

Security Training 47

Server Hardening 47

Software Licensing 49

System Development 49

Vendor Access 50

Virus Protection 52

Violation Notice 54

References 54

Acknowledgement 55

INTRODUCTION

This Security Policy is a mechanism used to establish the limits and expectations for the users of the Town of Beekman, New York computer network and provides the baseline for implementing security controls to reduce both vulnerabilities and risk. Internal users should have no expectation of privacy with respect to Information Technology. The purpose of the Town of Beekman, New York Security Policy is to clearly communicate the Town's information security expectations to Town employees and elected & appointed officials who use Town equipment and access the Town network. This Policy applies equally to all individuals who use any Town of Beekman, New York Information Resources. Electronic files created, sent, received, or stored on computers owned, leased, administered, or otherwise under the custody and control of the Town of Beekman are the property of the Town of Beekman. This Security Policy is supported by the following Security Policy Standards:

1) IT Security controls must not be bypassed or disabled.

2) Security awareness of personnel must be continually emphasized, reinforced, updated and validated.

3) All personnel are responsible for managing their use of IR and are accountable for their actions relating to IT security.

4) Passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and other computer systems security procedures and devices shall be protected by the individual user from use by, or disclosure to, any other individual or organization. All security violations shall be reported to the Town Board and Designated IT official.

5) Access to, change to, and use of IR must be strictly secured. Information access authority for each user must be reviewed on a regular basis, as well as each job status change such as: a transfer, promotion, demotion, or termination of service.

6) The use of IT must be for officially authorized business purposes only. There is no guarantee of personal privacy or access to tools such as, but not limited to; email, web browsing, and other electronic discussion tools. The use of these electronic communications tools may be monitored to fulfill compliance or investigative requirements.

7) Departments responsible for the custody and operation of computers shall be responsible for proper authorization of IR utilization, the establishment of effective use, and reporting of performance issues to the designated IT official.

8) Any data used in an IR system must be kept confidential and secure by the user. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and secure. Furthermore if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured according to the New York State Archives directives.

9) Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the Town Board and designated IT official.

10) On termination of the relationship with the Town, users must surrender all property and IR managed by the Town. All security policies for IR apply to and remain in force in the event of a terminated relationship until such surrender is made. Further, this policy survives the terminated relationship.

11) The owner must communicate to the Designated IT official, the intent to acquire any computer hardware or to purchase or computer software. The costs of acquisitions, development and operation of computer hardware and applications must be part of the designated IT official budget and authorized by the Town Board.

12) The department which requests and authorizes a computer application must take the appropriate steps to ensure the integrity and security of all programs and data files created by, or acquired for, computer applications. To ensure a proper segregation of duties, Administrative responsibilities cannot be delegated to the users.

13) The Town network is owned by the Town of Beekman and controlled by the designated IT official.

14) Approval must be obtained from the designated IT official before connecting a device that does not comply with published guidelines to the network.

15) The designated IT official reserves the right to remove any network device that does not comply with standards or is not considered to be adequately secure.

16) The sale or release of computer programs or data, including email lists and departmental telephone directories, to other persons or organizations must comply with all Town legal and fiscal policies and procedures.

17) The integrity of general use software, utilities, operating systems, networks, and respective data files are the responsibility of the designated IT official. Data for test and research purposes must be de-personalized prior to release to testers unless each individual involved in the testing has authorized access to the data.

18) All changes to IR systems, networks, programs or data must be approved by the designated IT official to preserve its integrity.

19) Individual departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the reporting any suspected or confirmed violations of this policy to the appropriate management.

20) All departments must carefully assess the risk of unauthorized alteration, unauthorized disclosure, or loss of the data for which they are responsible and ensure, through the use of monitoring systems, that the Town is protected from damage, monetary or otherwise. The designated IT official must have appropriate backup and contingency plans for disaster recovery based on risk assessment and Town business requirements.

21) All computer systems contracts, leases, licenses, consulting arrangements or other agreements must be authorized and signed by the Town Supervisor as directed by the Town Board. These arrangements must contain terms approved as to form by the Town’s Legal counsel, advising vendors of Town’s IR retained proprietary rights and acquired rights with respect to its information systems, programs, and data requirements for computer systems security, including data maintenance and return.

22) IR computer systems and/or associated equipment used for Town business that is conducted and managed outside of Town control must meet Security Policy requirements and be subject to monitoring.

23) External access to and from IR must meet appropriate published Town security guidelines.

24) All commercial software used on computer systems must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product. Personnel must abide by all license agreements and must not illegally copy licensed software. The designated IT official reserves the right to remove any unlicensed software from any computer system.

Definitions:

Abuse of Privilege: When a user willfully performs an action prohibited by organizational policy or law, even if technical controls are insufficient to prevent the user from performing the action.

Application Software: A program or group of programs designed for end users. Application software can be divided into two general classes: systems software and applications software. Systems software consists of low-level programs that interact with the computer at a very basic level. This includes operating systems, compilers, and utilities for managing computer resources.

Applied Computer Systems: Both hardware and software, and often including networking and telecommunications, usually in the context of a business or other enterprise. Often this is the name of the part of an enterprise that deals with all things electronic.

Backup: Copy of files and applications made to avoid loss of data and facilitate recovery in the event of a system crash**.**

Custodian: Guardian or caretaker; the holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information.
For mainframe applications, The designated IT official is the custodian; for micro and mini applications, the owner or user may retain custodial responsibilities.

Electronic mail system: Any computer software application that allows electronic mail to be communicated from one computing system to another.

Electronic mail (email): Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

E-mail: Abbreviation for electronic mail, which consists of messages sent over any electronic media by a communications application.

Help Desk: Resource provided by the Town of Beekman to assist users with managing their computer and peripheral issues.

Information: Any and all data, regardless of form, that is created, contained in, or processed by, Information Resources facilities, communications networks, or storage media.

Information Management (IM): The manipulation, re-organization, analysis, graphing, charting, and presentation of data for specific management and decision-making purposes.

Information Resource (IR): Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Technology (IT): Includes all matters concerned with the furtherance of computer science and technology and with the design, development, installation, and implementation of information systems and applications.

IT Asset: Any Town-owned information, system or hardware that is used in the course of business activities.

Information Security Officer (ISO): Responsible to the Town Board for administering the information security functions within the Town. The ISO and the Town Supervisor is the Town's internal and external point of contact for all information security matters.

Internet: A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and colleges. The Internet is the present "information superhighway."

Intranet: A private network for communications and sharing of information that, like the Internet, is based on TCP/IP, but is accessible only to authorized users within an organization. An organization's intranet is usually protected from external access by a firewall.

Local Area Network (LAN): A data communications network spanning a limited geographical area, a few miles at most.

It provides communication between computers and peripherals at relatively high data rates and relatively low error rates.

Offsite Storage: Based on data criticality, offsite storage should be in a geographically different location from the Town Hall that does not share the same disaster threat event. Based on an assessment of the data backed up, removing the backup media from the building and storing it in another secured location at Town Hall may be appropriate.

Owner: The manager or agent responsible for the function which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments.

Password: A string of characters which serves as authentication of a person's identity, which may be used to grant, or deny, access to private or shared data.

PCI Compliance: Payment card industry (PCI) compliance is adherence to a set of specific security standards that were developed to protect card information during and after a financial transaction. PCI compliance is required by all card brands.

Portable Computing Devices: Any easily portable device that is capable of receiving and/or transmitting data to and from IR. These include, but are not limited to, notebook computers, handheld computers, PDAs, pagers, and cell/smart phones.

Security Incident: In information operations, an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent.

Server: A computer program that provides services to other computer programs in the same, or another, computer. A computer running a server program is frequently referred to as a server though it may also be running other client (and server) programs.

Strong Passwords: A strong password is a password that is not easily guessed. It is normally constructed of a sequence of characters, numbers, and special characters, depending on the capabilities of the operating system. Typically the longer the password the stronger it is.

It should never be a name, dictionary word in any language, an acronym, a proper name, a number, or be linked to any personal information about you such as a birth date, social security number, and so on.

System Development Life Cycle (SDLC): a set of procedures to guide the development of production application software and data items. A typical SDLC includes design, development, maintenance, quality assurance and acceptance testing.

Town Board: Shall be defined in this document as the majority vote of the Town Board including the Supervisor.

Town Calendar: Lists all approved meetings and events and is maintained by the Town Clerk.

Trojan Horse: Destructive programs—usually viruses or worms—that are hidden in an attractive or innocent-looking piece of software, such as a game or graphics program. Victims may receive a Trojan horse program by e-mail or on a diskette, often from another unknowing victim, or may be urged to download a file from a Web site or bulletin board.

User: An individual or automated application or process that is authorized access to the resource by the owner, in accordance with the owner’s procedures and rules.

Vendor: Someone who exchanges goods or services for money.

Virus: A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft Office programs that allow users to generate macros.

Webserver: A computer that delivers (*serves up*) web pages.

Web page: A document on the World Wide Web. Every Web page is identified by a unique URL (Uniform Resource Locator).

World Wide Web: A system of Internet hosts that supports documents formatted in HTML (Hypertext Markup Language) which contains links to other documents (hyperlinks) and to audio, video, and graphic images. Users can access the Web with special applications called browsers, such as Netscape Navigator, and Microsoft Internet Explorer.

Website: A location on the World Wide Web, accessed by typing its address (URL) into a Web browser. A Web site always includes a home page and may contain additional documents or pages.

Worm: A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. The first use of the term described a program that copied itself benignly around a network using otherwise unused resources on networked machines to perform distributed computation. Some worms are security threats, using networks to spread themselves against the wishes of the system owners, and disrupting networks by overloading them. A worm is similar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors at all.

Data Classification:

Data Classification provides a framework for managing data assets based on value and associated risks and for applying the appropriate levels of protection as required by New York State and federal law as well as proprietary, ethical, operational, and privacy considerations. All Town data, whether electronic or printed, should be classified as per the Town Records Management law and New York State Records Management and Retention Schedule MU1. Consistent use of data classification reinforces with users the expected level of protection of Town data assets in accordance with Town of Beekman Security Policy.

Purpose:

The purpose of Data Classification is to provide a foundation for the development and implementation of necessary security controls to protect information according to its value and/or risk.

Security standards, which define these security controls and requirements, may include: document marking/labeling, release procedures, privacy, transmission requirements, printing protection, computer display protections, storage requirements, destruction methods, physical security requirements, access controls, backup requirements, transport procedures, encryption requirements, and incident reporting procedures.

Data Classification practices apply equally to all individuals who use or handle any Town Information Resource.

Data shall be classified as follows:

SENSITIVE: This classification applies to information that requires special precautions to assure the integrity of the information, by protecting it from unauthorized modification or deletion. It is information that requires a higher than normal assurance of accuracy and_completeness. Sensitive information might include organization financial transactions and regulatory actions such as data that may be subject to disclosure or release under the New York Freedom of Information Act, but requires additional levels of protection.

- Examples of “Town-Sensitive” data may include but are not limited to:
- Town operational information
- Town personnel records
- Town information security procedures
- Town internal communications

CONFIDENTIAL: This classification applies to the most sensitive business information that is intended strictly for use within the organization. This information is exempt from disclosure under the provisions of the Freedom of Information Act or other applicable federal laws or regulations. Its unauthorized disclosure could seriously and adversely impact the Town and/or its residents, For example, Birth and Death Certificates and related information should be considered at least CONFIDENTIAL. Examples of “Confidential” data may include but are not limited to:

- Personally Identifiable Information, such as: a name in combination with Social Security Number (SSN) and/or financial account numbers
- Intellectual Property, such as: Copyrights, Patents and Trade Secrets

PRIVATE: This classification applies to personal information that is intended for use within the Town of Beekman offices. Its unauthorized disclosure could seriously and adversely impact the Town and/or its employees.

PUBLIC: This classification applies to all other information that does not clearly fit into any of the above three classifications. While its unauthorized disclosure is against policy, it is not expected to impact seriously or adversely the Town, its employees, and/or its residents.

POLICY AREAS:

Acceptable Use: Under the provisions of the New York State Cyber Security Policy P03-002, Information Resources are strategic assets of Government Agencies including Local Governments that must be managed as valuable resources. Thus this policy is established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of information resources.
- To educate individuals who may use information resources with respect to their responsibilities associated with such use.

This policy area applies equally to all individuals granted access privileges to any Town Information Resources. Electronic files created, sent, received, or stored on Information Resources owned, leased administered, or otherwise under the custody and control of the designated IT official are the property of the Town of Beekman. Electronic files created, sent, received, or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of the Town are not private and may be accessed by the designated IT official at any time without knowledge of the Information Resources user or owner.

Electronic file content may be accessed by appropriate personnel for maintenance purposes and with the authorization of the Supervisor or Town Board in the event of security related matters.

- Users must report any weaknesses in Town computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the designated IT official.
- Users must not attempt to access any data or programs contained on Town systems for which they do not have authorization or explicit consent.

- Users must not divulge Dial-up or Dial-back modem phone numbers to anyone.
- Users must not share their Town account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes.
- Users must not make unauthorized copies of copyrighted software.
- Users must not use non-standard shareware or freeware software without designated IT official approval.
- Users must not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of Information Resources; deprive an authorized Town user access to a Town resource; obtain extra resources beyond those allocated or circumvent Town computer security measures.
- Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system.

  For example, Town users must not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on Town Information Resources.
- Town Information Resources must not be used for personal benefit.
- Users must not intentionally access, create, store or transmit material which the Town may deem to be offensive, indecent or obscene.
- Access to the Internet from a Town owned, home based, computer must adhere to all the same policies that apply to use from within Town facilities. Employees must not allow family members or other non-employees to access Town computer systems.
- Users must not otherwise engage in acts against the aims and purposes of the Town as specified in its governing documents or in rules, regulations and procedures adopted from time to time.
- As a convenience to the Town user community, incidental use of Information Resources is permitted. The following restrictions apply:
  - ❖ Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, and so on, is restricted to Town approved users; it does not extend to family members or other acquaintances.

- ❖ Incidental use must not result in direct costs to the Town.
- ❖ Incidental use must not interfere with the normal performance of an employee’s work duties.
- ❖ No files or documents may be sent or received that may cause legal action against, or embarrassment to the Town.
- ❖ Storage of personal email messages, voice messages, files and documents within the Town’s Information Resources must be nominal.
- ❖ All messages, files and documents – including personal messages, files and documents – located on Town Information Resources are owned by the Town, may be subject to open records requests, and may be accessed in accordance with this policy.

Account Management: Computer accounts are the means used to grant access to the Town’s Information Technology. These accounts provide a means of providing accountability, a key to any computer security program, for IT usage. This means that creating, controlling, and monitoring all computer accounts is extremely important to an overall security program. The purpose of this policy area is to establish the rules for the creation, monitoring, control and removal of user accounts and applies equally to all individuals with authorized access to any Town Information Resource.

- All accounts created must have an associated request and approval that is appropriate for the Town’s system or service.
- All users must sign the Town of Beekman Computer Use Policy and Town of Beekman Security Policy Acknowledgements and before access is given to an account.
- All accounts must be uniquely identifiable using the assigned user name.
- All default passwords for accounts must be constructed in accordance with this Security Policy.
- All accounts must have a password expiration that complies with this Security Policy.
- Accounts of individuals on extended leave (more than 30 days) will be disabled.
- All new user accounts that have not been accessed within 30 days of creation will be disabled.
- IT Designated Officials:

- Are responsible for removing the accounts of individuals that change roles within the Town or are separated from their relationship with the Town.

- Must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes.

- Must have a documented process for periodically reviewing existing accounts for validity.

- Are subject to independent audit review by the Town Board.

- Must provide a list of accounts for the systems they administer when requested by the Town Board.

- Must cooperate with the Supervisor and/or Town Board when investigating security incidents.

Administrative/Special Access: Technical support staff and others designated by the Beekman Town Board may have special access account privilege requirements compared to typical or everyday users. The fact that these administrative and special access accounts have a higher level of access means that granting, controlling and monitoring these accounts is extremely important to an overall security program. The purpose of the policy area is to establish the rules for the creation, use, monitoring, control and removal of accounts with special access privilege and applies equally to all individuals that have, or may require, special access privilege to any Town information resources.

- The designated IT official must keep a list of user access account privileges for software connected to the Town network.

- All users must sign the Town of Beekman Computer Use Policy and Town of Beekman Security Policy Acknowledgement before access is given to an account.

- All users of Administrative/Special access accounts must have account management instructions, documentation, training, and authorization.

- Each individual that uses Administrative/Special access accounts must refrain from abuse of privilege and must only do investigations under the direction of the Supervisor and/or Town Board.

- Each individual that uses Administrative/Special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
- Each account used for administrative/special access must meet this Security Policy.
- The password for a shared administrator/special access account must change when an individual with the password leaves the department or Town or upon a change in the vendor personnel assigned to the Town contract.
- In the case where a system has only one administrator there must be a password escrow procedure in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.
- When Special Access accounts are needed for Internal or External Audit, software development, software installation, or other defined need, they:
    - must be authorized by the Town Board
    - must be created with a specific expiration date
    - must be removed when work is complete

Asset Management: Information technology (IT) asset management provides for policies, procedures, and guidelines for lifecycle management of the Town of Beekman's IT assets from standards and acquisition to installations, management, and surplus. The purpose of this policy area is to establish the rules for the creation, monitoring, control and removal of Town IT Assets and applies equally to all individuals with authorized access to any Town Information Resource. The Town uses information technology (IT) to assist Town departments and Boards in conducting official Town business by following the rules set forth below:

Policy Mandates:

- The designated IT official is responsible for the management of IT assets and lifecycle processes, including standards, acquisition, management, surplus, and long-range planning.
- Consistency in technology allows the development of efficient and cost-effective methods for supporting and managing the technology environment and in planning for upgrades, migrations, staff training, and future technology installations. Long-range planning for information technology changes shall include business as well as technical input.
- IT acquired for or on behalf of the Town is owned by the Town of Beekman.
- IT equipment is assigned to the position, not the individual, and remains with the position if the individual terminates employment or is transferred to another position. If a position is abolished, IT equipment will be returned to designated IT official inventory.
- IT equipment will be used within the Town as long as practicable.
- Employees who violate or otherwise abuse the provisions of this policy may be subject to disciplinary action, up to and including dismissal.

Acquisitions:

- Acquisition of all information technology for the Town is the responsibility of the designated IT official as approved in the adopted budget by the Town Board.
- Acquisition of IT shall follow the Purchasing Policy. Purchases, contracts, amendments, and renewals will be processed through the designated IT official for approval by the Town Board.
- Approvals for acquisition are based on availability of funds as determined by the Town Board, conformance to IT standards, and solution match for department need.
- All IT acquired for or on behalf of the Town or developed by designated IT official employees or contract personnel on behalf of the Town are and shall be deemed Town of Beekman property.

Standards:

- A standard, basic technical infrastructure will be established for the Town. It will be defined and managed by the designated IT official and will include the network and the desktop.
- Desktop IT consists of standard hardware and software configurations and images (excluding test computers).

- The designated IT official is responsible for:
  - Establishing hardware and software standards for any IT product.
  - Reviewing requests for new, amended, or replacement IT standards. New-to-Town IT will be assessed by designated IT official staff for compatibility with and impact on other Town IT components, as appropriate.
  - Using department-wide business and technical needs in determining approval of new, amended, or replacement standards.
  - Establishing standard software configurations and desktop images. These standards shall automate business rules where possible (e.g. use of screen saver password protection).
  - New IT policy and standard decisions shall have formal plans for implementation.

Equipment Management:

- The Town of Beekman will control its IT assets to comply with State policies and regulations, as well as applicable licensing and copyright laws.
- The designated IT official is responsible for tracking Town-owned software and hardware, including licenses, through an inventory control system. Software inventory records and reports shall be available for audit at any time.

Installations of Software and Hardware:

- The Town shall maintain an IT environment whereby installations and configurations are centrally managed through the Designated IT official.
- Only Town designated standard software, hardware, or approved exception shall be installed.
- Software, hardware, or approved exception must be Town owned or licensed. All software without required licenses will be removed from the desktops/laptops.
- The Town ISO shall authorize installations of software, hardware, or approved exception.
- Installation of business-related, no cost software (i.e. Adobe Acrobat Reader or browser-required applications) shall be approved through

the designated IT official. These types of software shall be evaluated through the standards and exception to standards procedures.

- User-supplied software shall not be installed or executed on Town-owned desktops. Do not install or connect non-Town hardware to a Town of Beekman network.
- Unauthorized duplication of licensed software is a violation of this policy and a violation of copyright laws.
- All excess IT equipment within the Town shall be the responsibility of the designated IT official to reuse or surplus as determined by the designated IT official and Town Board. First priority for redeployment requests within the Town shall be by designated IT official determination.
- The designated IT official shall delete all data and applications, exclusive of the operating system, from all excess IT equipment prior to re-deployment or placing in spare inventory, loans, or surplus.
- The designated IT official shall be responsible for delivery of equipment to the identified re-deployment work site.
- The designated IT official shall store spare IT equipment in a designated reserve location for use as needed.

Exceptions:

- The Town Board is responsible for reviewing and approving exceptions to IT policies.
- The Town Board may grant exceptions to this policy under extraordinary circumstances. Requests for exceptions must be made in writing to the designated IT official stating the business need and unique circumstances requiring an exception.
- The Town Board and the ISO will evaluate and determine if the requested exception can be reasonably resolved through technology within the confines of the Town technology environment and the security of the Town network.
- For granted exceptions, the requester must establish with the designated IT official a plan for technical support, training, and maintenance. The plan shall be developed prior to purchase or implementation of non-standard technology.
- Exceptions shall be considered provisional and can be superseded any time a Town standard is determined.
- If a broader need is determined at the time of an exception request, then a Town standard will be established.

- Upon granting an exception regarding access to or connection with the Town local or wide area network, a written agreement between the requester and designated IT official must be developed stating the conditions of access, security, technical support, and maintenance.

IT Equipment Loans:

- Only spare IT equipment that is no longer under warranty is eligible for loan to Town partners or associates. Loaned IT equipment is allowed in situations where the Town Board determines that the loan to a partner or associate will fulfill the Towns' mission or goals.
  Loan of equipment will comply with policies, rules, regulations, and laws governing State or Town owned IT equipment.
- Conditions of each loan shall include but are not limited to the following:
  - ❖ The designated IT official shall delete all data and applications, exclusive of operating system, residing on loan IT equipment.
  - ❖ Loan IT equipment shall remain on Town IT asset and inventory records.
  - ❖ The designated IT official is responsible for completion of a loan agreement with the user
  - ❖ The user of the loan IT equipment shall be responsible for any physical damage or loss, ordinary wear and tear excepted, regardless of fault.
  - ❖ The designated IT official is not responsible for maintenance or repair of loan IT equipment, including hardware, software, or connectivity.

Surplus:

- The designated IT official shall delete all data and applications, exclusive of operating system, residing on surplus IT equipment. The designated IT official shall process the surplus IT equipment and obtain a certified Town Board Resolution for all equipment surplus.

Back Up: Electronic backups are a business requirement to enable the recovery of data and applications in the case of events such as natural disasters, system disk drive failures, espionage, data entry errors, or system operations errors.

The purpose of this policy area is to establish the rules for the backup and storage of electronic Town information and applies to all individuals within the Town that are responsible for the installation and support of Information Resources and individuals charged with Information Security. The designated IT official may have existing contracts for offsite backup data storage. These services can be extended to all Town entities upon request.

- The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the Town.
- The Town Information Resources backup and recovery process for each system must be documented and periodically reviewed.
- The vendor(s) providing offsite backup storage for the Town must be cleared to handle the highest level of information stored.
- Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally backup media must be protected in accordance with the highest Town of Beekman sensitivity level of information stored.
- A process must be implemented to verify the success of the Town electronic information backup.
- Backups must be periodically tested to ensure that they are recoverable.
- Contracts held by the offsite backup storage vendor(s) for access to the Town backup media must be reviewed annually or when an authorized individual leaves the Town.
- Procedures between the Town and the offsite backup storage vendor(s) must be reviewed at least annually.
- All Off-site back up contracts must be approved by the New York State Commissioner of Education pursuant to section 185.9 of the Regulations of the Commissioner of Education.
- Backup tapes must have at a minimum the following identifying criteria that can be readily identified by labels and/or a bar-coding system:
    - ❖ System name
    - ❖ Creation Date

- Sensitivity Classification [Based on the New York State Records management MU-1 Schedule]

- Town of Beekman Contact Information

Court Information Resources: The Town of Beekman recognizes the unique circumstances that separate Beekman Court Information Resources from Town Information Resources. This policy area is established to ensure compliance with both Town and New York State Unified Court Information Resources.

New York State Unified Court hardware in the form of workstations, laptops and monitors are used by Beekman Court Judges and personnel and are authorized by this policy to be integrated with the Town network owned and maintained by the Town of Beekman. Court electronic records are stored locally on non-Town owned workstations and it is the Court’s responsibility to ensure that backups are made and workstations are maintained per the NYS Office of Court Administration.

Email: This policy area is established to ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources. It establishes prudent and acceptable practices regarding the use of email and will educate individuals using email with respect to their responsibilities associated with such use.

The purpose of the this policy area is to establish the rules for the use of Town email for the sending, receiving, or storing of electronic mail and applies equally to all individuals granted access privileges to any Town information resource with the capacity to send, receive, or store electronic mail The following activities are prohibited by this policy:

- Sending email that is intimidating or harassing.
- Using email for conducting personal business.
- Using email for purposes of political lobbying or campaigning.
- Violating copyright laws by inappropriately distributing protected works.
- Posing as anyone other than oneself when sending email, except when authorized to send messages for another when serving in an administrative support role.
- The use of unauthorized e-mail software.

- The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:
    - Sending or forwarding chain letters
    - Sending unsolicited messages to groups in excess of 35 email addresses
    - Sending excessively large messages
    - Sending or forwarding email that is likely to contain computer viruses

- All user activity on Town Information Resource assets is subject to logging and review.

- All sensitive Town material transmitted over external network must be encrypted.

- Electronic mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the Town or any department of the Town unless appropriately authorized (explicitly or implicitly) to do so.

Where appropriate, an explicit disclaimer will be included unless it is clear from the context that the author is not representing the Town. An example of a simple disclaimer is: "the opinions expressed are my own, and not necessarily those of my employer."

- Individuals must not send, forward or receive confidential or sensitive Town information through non-Town email accounts. Examples of non-Town email accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, Optonline and email provided by other Internet Service Providers (ISP).

- The Town of Beekman must comply with the Federal Anti-Spam Act of 2003. Town officials and employees with active email addresses must:

    - ❖ Refrain from sending same subject email to more than 10 recipients outside of the Town of Beekman domain from their Outlook, Third party application (such as Blackberry Internet Service, IPhone or Android email services) or email server.

    - ❖ All mass email communications sent on behalf of the Town must be sent through the Town's email marketing service.

Help Desk: The Town of Beekman has installed a Help Desk system whereby users with computer issues or questions can open a ticket and the Town's computer consultant will respond and assist them with their issue. In addition, users may request training for Town issued software thru the Help Desk system.

Incident Management: The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some the actions that can be taken to reduce the risk and drive down the cost of security incidents. This document describes the requirements for dealing with computer security incidents. Security incidents include, but are not limited to: virus, worm, and Trojan horse detection, unauthorized use of computer accounts and computer systems, as well as complaints of improper use of Information Resources as outlined in the Email, Internet, Acceptable Use Policy areas and apply equally to all individuals that use any Town Information Resources.

The purpose of this policy area is to establish the rules for the creation, monitoring, control and removal of user accounts and applies equally to all individuals with authorized access to any Town Information Resource.

- Required by New York State Town Law #899, The Town of Beekman Information and Security Notification Breach Policy was adopted on July 23, 2014 and is followed in conjunction with this policy area in the event of a Cyber Security incident.
- Whenever a security incident, such as a virus, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed, the appropriate Incident Management procedures must be followed.
- The ISO is responsible for notifying the Supervisor and Town Board and initiating the appropriate incident management action including restoration as defined in the Incident Management Procedures.
- The ISO is responsible for determining the physical and electronic evidence to be gathered as part of the Incident Investigation.
- The appropriate technical resources from the designated IT official are responsible for monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.

- The ISO, working with the Supervisor, will determine if a widespread Town communication is required, the content of the communication, and how best to distribute the communication.
- The appropriate technical resources from the designated IT official are responsible for communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.
- The ISO is responsible for initiating, completing, and documenting the incident investigation.
- The ISO is responsible for reporting the incident to the:
    - ❖ Supervisor
    - ❖ Town Board
    - ❖ Local, state or federal law officials as required by applicable statutes and/or regulations
- The ISO is responsible for coordinating communications with outside organizations and law enforcement.
- In the case where law enforcement is involved, the ISO will act as the liaison between law enforcement and the Town.

Inter-Municipal Agreement for IT Shared Services: This policy area outlines the responsibilities for both the Town of Beekman and the Town of Dover with respect to an Information Technology Shared Services agreement.

INTERMUNICIPAL AGREEMENT BETWEEN THE TOWN OF BEEKMAN AND THE TOWN OF DOVER – PROVIDING COOPERATIVE INFORMATION TECHNOLOGY SERVICES

THIS AGREEMENT, made and entered into this 27th day of August, 2014, between the Town of Beekman, a municipal subdivision of the State of New York situate in Dutchess County, New York located at 4 Main Street, Poughquag, New York and the Town of Dover, a municipal subdivision of the State of New York, situate in Dutchess County, New York, located at 126 East Duncan Hill Road, Dover Plains, New York,

WITNESSETH:

WHEREAS, The Town of Dover currently employs staff within its municipality to oversee the day to day operations of the Town's computers, servers, peripherals, network infrastructure, email, software applications and hardware, Geographic Information Systems (GIS), radio communications, telecommunications technology, project management as well as the Town website and television station, and;

WHEREAS, the Town of Beekman is desirous of contracting with the Town of Dover for the purpose of utilizing the Town of Dover's Information Technology staff on an "as needed" basis in the maintenance and oversight of the Town of Beekman's computers, servers, peripherals, network infrastructure, software applications and hardware,

NOW, THEREFORE, IT IS HEREBY AGREED, by the Town of Beekman and the Town of Dover as follows:

1. The Town of Dover hereto authorizes its Principal Clerk for Information Technology and Information Technology staff to provide resources including equipment, facilities, purchasing authority and personnel ("Information Technology Services") to the Town of Beekman, pursuant to the terms attached hereto and made part of **Exhibit A**, subject to the following conditions.

2. The Information Technology services are strictly voluntary and should not in any way hamper or delay the Information Technology services and/or work within the Town of Dover.

3. The Town of Dover shall keep records of work performed, the days and hours (as appropriate) that Information Technology services were used and provide copies of this documentation to the Town of Beekman for verification and reimbursement on a monthly basis via the Town of Dover Help Desk.

4. The Town of Beekman shall make whole the Town of Dover for any and all expenses incurred by the Town of Dover on behalf of the Town of Beekman on a monthly basis.

5. The Town of Beekman shall be responsible for coordinating the efficient use of the Town of Dover Information Technology staff and be responsible for releasing said personnel as soon as possible. The Town of Dover shall retain full control over the management and assignments of its Information Technology staff.

6. The Town of Beekman authorizes the Town of Dover to act on its behalf in the execution within the scope of services outlined in this agreement dealing with vendors, service providers or other government agencies.

7. The term of this agreement shall end on December 31, 2014 and may be replaced with a new agreement containing details of any shared services grant received.

8. Both parties agree to obtain and thereafter keep in full force and effect their general liability insurance, public liability insurance, and automotive insurance relative to the various services performed herein with limits of not less than $1,000,000 per occurrence and $1,000,000 annual aggregate.

9. Both parties agree to obtain and thereafter update and keep in full force and effect their Security Policy, Computer Use Policy and Information and Security Breach Notification Policy.

10. Should any dispute arise between both parties respecting the terms of this agreement, the disputed matter shall be settled by arbitration in accordance with the laws of the State of New York.

11. In accordance with the provisions of section 109 of the General Municipal Law, both parties hereto are prohibited from assigning, transferring, conveying, subletting or otherwise disposing of this agreement, or of its right, title or interest in this agreement to any other person or corporation without the previous consent in writing of the other party.

12. The Town Supervisor of the Town of Dover has executed this agreement pursuant to a resolution adopted by the Town Board of the Town of Dover, at a meeting held on July 30th, 2014. Ryan Courtien, Town Supervisor, whose signature appears hereafter, is duly authorized and empowered to enter into such agreement on behalf of the Town of Dover. This instrument shall be executed in duplicate. At least one copy shall be permanently filed, after execution thereof, with the Town Clerk of Town of Dover.

13. The Town Supervisor of the Town of Beekman has executed this agreement pursuant to a resolution adopted by the Town Board of the Town of Beekman, at a meeting held on September 3rd, 2014. Barbara Zulauf, Town Supervisor, whose signature appears hereafter, is duly authorized and empowered to enter into such agreement on behalf of the Town of Beekman. This instrument shall be executed in duplicate. At least one copy shall be permanently filed, after execution thereof, with the Town Clerk of Town of Beeekman.

14. Any notices and payments required hereunder shall be addressed as follows, or to such other address as may hereafter be designated in writing by either party hereto:

To the Town of Beekman:
Barbara Zulauf, Town Supervisor
4 Main Street
Poughquag, New York 12570

To the Town of Dover:
Ryan Courtien, Town Supervisor
126 East Duncan Hill Road
Dover Plains, New York 12522

15. No waiver of any breach of any condition of this agreement shall be binding unless in writing and signed by the party waiving the said breach. No such waiver shall in any way affect any other term or condition of this agreement or constitute a cause or excuse for a repetition of such or any other breach unless the waiver shall include the same.

16. This agreement constitutes the complete understanding of the parties. No modification of any provisions thereof shall be valid unless in writing and signed by both parties.

17. This agreement is governed by the laws of the State of New York.

IN WITNESS WHEREOF, THE TOWN OF, the Town of Dover has caused its corporate seal to be affixed hereto and these presents to be signed by Ryan Courtien, Supervisor, and the Town of Beekman has caused cause its corporate seal to be affixed hereto to these presents to be signed by Supervisor Barbara Zulauf. - Original agreement on file in both Town Clerk's office.

Internet: This policy area applies equally to all individuals granted access to any Town Information Resource with the capacity to access the internet, the intranet, or both and is established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of the internet.
- To educate individuals who may use the internet, the intranet, or both with respect to their responsibilities associated with such use.

• Software for browsing the Internet is provided to authorized users for business and research use only.

• All software used to access the Internet must be part of the Town's standard software suite or approved by the designated IT official. This software must incorporate all vendor provided security patches.

• All files downloaded from the Internet must be scanned for viruses using the approved designated IT official distributed software suite and current virus detection software.

• All software used to access the Internet shall be configured to use the firewall http proxy.

• All sites accessed must comply with the Acceptable Use policy area in this document.

• All user activity on Town Information Resources assets is subject to logging and review.

• Content on all Town Web sites must comply with the Acceptable Use policy area in this policy.

• No offensive or harassing material may be made available via Town Web sites.

• Non-business related purchases made over the internet are prohibited. Business related purchases are subject to Town procurement rules.

• No personal commercial advertising may be made available via Town Web sites.

• Town internet access may not be used for personal gain or non-Town personal solicitations.

• No Town data will be made available via Town Web sites without ensuring that the material is available to only authorized individuals or groups.

• All sensitive Town material transmitted over external network must be encrypted.

• Electronic files are subject to the same records retention rules that apply to other documents and must be retained in accordance with departmental records retention schedules.

Intrusion Detection: The Town of Beekman network infrastructure is provided as a central utility for all users of Town Information Resources. It is important that the infrastructure, which includes cabling and the associated 'active equipment', continues to develop with sufficient flexibility to meet Town demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services. The purpose of the policy area is to establish the rules for the access and use of the network infrastructure. These rules are necessary to preserve the integrity, availability and confidentiality of Town information apply equally to all individuals with access to any Town Information Resource.

- Users are permitted to use only those network addresses issued to them by the designated IT official.
- All remote access (dial in services) to the Town will be either through an approved modem pool or via an Internet Service Provider (ISP).
- Remote users may connect to Town Information Resources only through an ISP and using protocols approved by the Town.
- Users inside the Town firewall may not be connected to the Town network at the same time a modem is being used to connect to an external network.

- Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the Town network without designated IT official approval.
- Users must not install network hardware or software that provides network services without Designated IT official approval.
- Non-Town computer systems that require network connectivity must conform to Town Information Security Standards.
- Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, Town users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the Town network infrastructure.
- Users are not permitted to alter network hardware in any way

Network Access: The Town of Beekman network infrastructure is provided as a central utility for all users of Town Information Resources. It is important that the infrastructure, which includes cabling and the associated 'active equipment', continues to develop with sufficient flexibility to meet the Town's demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

The purpose of this policy area is to establish the rules for the access and use of the network infrastructure. These rules are necessary to preserve the integrity, availability and confidentiality of Town information.

The Town Network Access standards apply equally to all individuals with access to any Town Information Resource.

Network Access Standards are as follows:

- Users are permitted to use only those network addresses issued to them by the Town of Beekman designated IT official.
- All remote access (dial in services and broadband) to the Town will be either through an approved modem pool or via an Internet Service Provider (ISP).
- Remote users may connect to Town Information Resources only through an ISP and using protocols approved by the Town.

- Users inside the Town firewall may not be connected to the Town network at the same time a modem is being used to connect to an external network.
- Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the Town network without designated IT official approval.
- Users must not install network hardware or software that provides network services without designated IT official approval.
- Non-Town computer systems that require network connectivity must conform to Town of Beekman IT Standards.
- Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, Town users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the Town of Beekman Network infrastructure.
- Users are not permitted to alter network hardware in any way.

Network Configuration: The Town network infrastructure is provided as a central utility for all users of Town Information Resources. It is important that the infrastructure, which includes cabling and the associated equipment such as routers and switches, continues to develop with sufficient flexibility to meet user demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

The purpose of this policy area is to establish the rules for the maintenance, expansion and use of the network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of Town information applies equally to all individuals with access to any Town Information Resource.

- The Town of Beekman owns and is responsible for the Town network infrastructure and will continue to manage further developments and enhancements to this infrastructure.

- To provide a consistent municipal network infrastructure capable of exploiting new networking developments, all cabling must be installed by a contractor approved by the designated IT official.

- All network connected equipment must be configured to a specification approved by designated IT official.
- All hardware connected to the Town network is subject to designated IT official management and monitoring standards.
- Changes to the configuration of active network management devices must not be made without the approval of the designated IT official.
- The Town network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by the designated IT official.
- The networking addresses for the supported protocols are allocated, registered and managed centrally by the designated IT official.
- All connections of the network infrastructure to external third party networks are the responsibility of the designated IT official. This includes connections to external telephone networks.
- The use of departmental firewalls is not permitted without the written authorization from the designated IT official.
- Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the Town network without designated IT official approval.
- Users must not install network hardware or software that provides network services without designated IT official approval.
- Users are not permitted to alter network hardware in any way

Password: User authentication is a means to control who has access to an Information Resource system. Controlling the access is necessary for any Information Resource.

Access gained by a non-authorized entity can cause loss of information confidentiality, integrity and availability that may result in loss of revenue, liability, loss of trust, or embarrassment to the Town of Beekman. The purpose of this policy area is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of the Town user authentication mechanisms and applies equally to all individuals who use any Town information resources. Three factors, or a combination of these factors, can be used to authenticate a user. Examples are:

  - Something you know – password, Personal Identification Number (PIN)
  - Something you have – Smartcard
  - Something you are – fingerprint, iris scan, voice
  - A combination of factors – Smartcard and a PIN

- All passwords, including initial passwords, must be constructed and implemented according to the following Designated IT official rules:

  - ❖ It must be changed every 90 days
  - ❖ It must adhere to a minimum length as established by the designated IT official
  - ❖ It must be a combination of alpha and numeric characters
  - ❖ It must not be anything that can easily tied to the account owner such as: user name, social security number, nickname, relative’s names, birth date, etc.
  - ❖ Password history must be kept to prevent the reuse of a password

  - Stored passwords must be encrypted.
  - User account passwords must not be divulged to anyone. The designated IT official and its contractors will not ask for user account passwords.
  - Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with the Town (if applicable)
  - If the security of a password is in doubt, the password must be changed immediately.
  - Administrators must not circumvent this Policy for the sake of ease of use.
  - Users cannot circumvent password entry with auto logon, application remembering, embedded scripts or hardcoded passwords in client software. Exceptions may be made for specific applications (like automated backup, or when Windows Authentication is in use) with the

approval of the designated IT official. In order for an exception to be approved there must be a procedure to change the passwords.

- Computing devices must not be left unattended without enabling a password protected screensaver or logging off of the device.
- Password Guidelines:
    - Passwords must have a minimum length of 6 alphanumeric characters.
    - Passwords must contain a mix of upper and lower case characters and have at least 2 numeric characters. The numeric characters must not be at the beginning or the end of the password. Special characters should be included in the password where the computing system permits. The special characters are (!@#$%^&*_+=?/~`;:,<>|\).
    - Passwords must not be easy to guess and they:
        - Must not be your Username
        - Must not be your employee number
        - Must not be your name
        - Must not be family member names
        - Must not be your nickname
        - Must not be your social security number
        - Must not be your birthday
        - Must not be your license plate number
        - Must not be your pet's name
        - Must not be your address
        - Must not be your phone number
        - Must not be the name of your town or city
        - Must not be the name of your department
        - Must not be street names

        - Must not be makes or models of vehicles
        - Must not be obscenities
        - Must not be any information about you that is known or is easy to learn (favorite - food, color, sport, etc.)
    - Passwords must not be reused for 24 consecutive password changes
    - Passwords must not be shared with anyone
    - Passwords must be treated as confidential information
    - While a supervisor may request access to your data via proper channels, they may not request your password, nor should a user feel obliged to supply their password.
    - Tips for creating a strong password
        - Combine short, unrelated words with numbers or special characters. For example: eAt42peN
        - Make the password difficult to guess but easy to remember
        - Substitute numbers or special characters for letters. (But do not just substitute) For example:
        - livefish - is a bad password
        - L1veF1sh - is better and satisfies the rules, but setting a pattern of 1st letter capitalized, and i's substituted by 1's can be guessed
        - l!v3f1Sh - is far better, the capitalization and substitution of characters is not predictable
- IT Helpdesk password change procedures must include the following:
    - Authenticate the user to the helpdesk before changing password
    - Change to a strong password
    - The user must change password at first login

- In the event passwords are found or discovered, the following steps must be taken:
    - Take control of the passwords and protect them
    - Report the discovery to the Town Help Desk
    - Transfer the passwords to an authorized person as directed by the designated IT official

PCI Compliance: The Town of Beekman accepts credit cards for tax payments, recreation activities, Dog and conservation licenses and other Town Clerk services. Although the Town is classified as a third party merchant certain responsibilities are required to be performed in order to be PCI Compliant. They are as follows:

- Maintain a secure network;
- Maintain a firewall configuration to protect cardholder data;
- May *not* use vendor-supplied defaults for system passwords and other security parameters;
- Protect cardholder data:
    - Advise and train staff on which card holder information they may keep;
    - Advise and train staff on how to protect stored cardholder data.
- Cardholder data may not be processed across open, public networks;
- Maintain a vulnerability management program:
    - Use and regularly update anti-virus software;
    - Develop and maintain secure systems and applications.
- Implement strong access control measures by:
    - Restricting access to cardholder data by business need-to-know;
    - Assigning a unique ID to each person with computer access.
    - Restricting physical access to cardholder data as well as credit card terminals.
- Regularly monitor and test networks by:
    - Tracking and monitoring all access to network resources and cardholder data;
    - Regularly testing security systems and processes.
- Maintain and enforcing this information security policy

Physical Access: Technical support staff, security administrators, and others designated by the Town Board may have Information Technology physical facility access requirements as part of their function.

The granting, controlling, and monitoring of the physical access to IT facilities is extremely important to an overall security program The purpose of this policy area is to establish the rules for the granting, control, monitoring, and removal of physical access to Information Resource facilities and applies to all individuals within the Town that are responsible for the installation and support of Information Technology, individuals charged with Information Security, and data owners.

- All physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.
- Physical access to the Town Server Room must be documented and managed.
- All IT facilities must be physically protected in proportion to the criticality or importance of their function in the Town.
- Access to the Server Room must be granted only to Town support personnel and contractors, whose job responsibilities require access to that facility.
- Access keys and codes must not be shared or loaned to others.
- Access keys that are no longer required must be returned to the Comptroller. Keys must not be reallocated to another individual bypassing the return process.
- Lost or stolen access keys must be reported to the Comptroller.
- The Server Room access log must be kept by the Comptroller.
- The Comptroller must review access records for the Server Room on a periodic basis and investigate any unusual access.
- The designated IT official must remove access rights of individuals that change roles within the Town or are separated from their relationship with the Town.
- Visitors must be escorted in security code access controlled areas of Information Technology facilities.
- Signage for restricted access rooms and locations must be practical, yet minimal discernible evidence of the importance of the location should be displayed.

Portable Computing: Portable computing devices are becoming increasingly powerful and affordable. Their small size and functionality are making these devices ever more desirable to replace traditional desktop devices in a wide number of applications. However, the portability offered by these devices may increase the security exposure to groups using the devices.

The purpose of this policy area is to establish the rules for the use of mobile computing devices and their connection to the network. These rules are necessary to preserve the integrity, availability, and confidentiality of Town information and apply equally to all individuals that utilize Portable Computing devices and access Town Information Resources.

- Only Town approved portable computing devices may be used to access Town Information Resources.
- Portable computing devices must be password protected.
- Town data should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all sensitive Town data must be encrypted using approved encryption techniques.
- Town data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols along with approved encryption techniques are utilized.
- All remote access to the Town of Beekman network must be either through an approved modem pool or via an Internet Service Provider (ISP).
- Non-Town computer systems that require network connectivity must conform to Town IT Standards and must be approved in writing by the designated IT official and Town Board.
- Unattended portable computing devices must be physically secure. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.

Privacy: Privacy Policies are mechanisms used to establish the limits and expectations for the users of the Town's Information Technology. Internal users should have no expectation of privacy with respect to Information Technology. External users should have the expectation of complete privacy, except in the case of suspected wrongdoing, with respect to Information Technology.

The purpose of this policy area is to clearly communicate the Town’s privacy expectations with respect to Information Technology users and applies equally to all individuals who use any Town Information Resource.

- Electronic files created, sent, received, or stored on IT owned, leased, administered, or otherwise under the custody and control of the Town of Beekman Domain are not private and may be accessed by the Town of Beekman designated IT official, with the permission on the Town Supervisor or for general maintenance at any time without knowledge of the user.
- To manage systems and enforce security, the Town of Beekman may log, review, and otherwise utilize any information stored on or passing through its IT systems in accordance with the provisions and safeguards provided in this Security Policy. For these same purposes, the Town of Beekman may also capture user activity such as telephone numbers dialed and web sites visited.
- A wide variety of third parties have entrusted their information to the Town of Beekman to provide Municipal services to the public, and all employees, and elected and appointed officials at working on behalf of the Town of Beekman be must do their best to safeguard the privacy and security of this information. The most important of these third parties is the individual customer; customer account data is accordingly confidential and access will be strictly limited based on Municipal need for access.
- Users must report any weaknesses in the Town of Beekman computer security, any incidents of possible misuse or violation of this agreement to the proper authorities and must comply with the Town of Beekman Information and Security Breach Notification Policy.
- Users must not attempt to access any data or programs contained on Town systems for which they do not have authorization or explicit consent.

Security Monitoring: Security Monitoring is a method used to confirm that the security practices and controls in place are being adhered to and are effective. The purpose of this policy area is to ensure that Information Resource security controls are in place, are effective, and are not being bypassed. One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities.

This early identification can help to block the wrongdoing or vulnerability before harm can be done, or at least to minimize the potential impact. Other benefits include Audit Compliance, Service Level Monitoring, Performance Measuring, Limiting Liability, and Capacity Planning and applies to all individuals that are responsible for the installation of new Information Resources, the operations of existing Information Resources, and individuals charged with Information Resource Security. Monitoring consists of activities such as the review of:

    - Automated intrusion detection system logs
    - Firewall logs
    - User account logs
    - Network scanning logs
    - Application logs
    - Data backup recovery logs
    - Help desk logs
    - Other log and error files

- Automated tools will provide real time notification of detected wrongdoing and vulnerability exploitation. Where possible a security baseline will be developed and the tools will report exceptions. These tools will be deployed to monitor:
    - Internet traffic
    - Electronic mail traffic
    - LAN traffic, protocols, and device inventory
    - Operating system security parameters
- The following files will be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:
    - Automated intrusion detection system logs
    - Firewall logs
    - User account logs

  - Network scanning logs
  - System error logs
  - Application logs
  - Data backup and recovery logs
  - Help desk trouble tickets
  - Telephone activity – Call Detail Reports
  - Network printer and fax logs

- The following checks will be performed at least annually by assigned individuals:
  - Password strength
  - Unauthorized network devices
  - Unauthorized personal web servers
  - Unsecured sharing of devices
  - Unauthorized modem use
  - Operating System and Software Licenses
  - Any security issues discovered will be reported to the Supervisor and Town Board for follow-up investigation.

Security Policy Standards: This policy area applies to all information obtained, created, or maintained by the Town's Information Technology. These Policy Standards are based on the interpretation of New York State's Cyber Security Policy P03-002 and other reference material and apply equally to all personnel including, but not limited to employees, agents, consultants, volunteers, Town Board, Elected and Appointed Officials and the personnel they supervise. Further, these Policy Standards apply to all information generated by the Town's Information Technology functions, through the time of its transfer to ownership external to the Town or its proper disposal/destruction.

- Application of Policy Standards
    - The designated IT official will protect the Information Resources assets of the Town of Beekman in accordance with the New York State Cyber Security Policy P02-003 and as authorized by the Town Board.
    - Specifically, the Town will apply policies, procedures, practice standards, and guidelines to protect its IR functions from internal data or programming errors and from misuse by individuals within or outside the Town.
        - This is to protect the Town from the risk of compromising the integrity of state programs, violating individual rights to privacy and confidentiality, violating criminal law, or potentially endangering the public's safety.
    - All Town Information Resources security programs will be responsive and adaptable to changing technologies affecting Information Resources
- Violations:
    - Any event that results in theft, loss, unauthorized use, disclosure, modification or destruction, or degraded or denied services of IR constitutes a breach of security and confidentiality. Violations may include, but are not limited to any act that:
        - exposes the Town to actual or potential monetary loss through the compromise of Information Resources security
        - involves the disclosure of sensitive or confidential information or the unauthorized use of Town data or resources
        - involves the use of Information Resources for personal gain, unethical, harmful, or illicit purposes, or results in public embarrassment to the Town.

Security Training: Understanding the importance of computer security and individual responsibilities and accountability for computer security are paramount to achieving organization security goals. This can be accomplished with a combination of general computer security awareness training and targeted, product specific training. The philosophy of protection and specific security instructions needs to be taught to, and re-enforced with, computer users. The security awareness and training information needs to be continuously upgraded and reinforced.

The purpose of this policy area is to describe the requirements to ensure each user of the Town’s Information Resources receives adequate training on computer security issues and applies equally to all individuals that use any Town Information Resource.

- All new users must attend an approved Security Awareness training class prior to, or at least within 30 days of, being granted access to any Town information resource.
- All users must sign an acknowledgement stating they have read and understand the Town of Beekman Computer Use Policy and the Town of Beekman Security Policy.
- All users (employees, consultants, contractors, temporaries, etc.) must be provided with sufficient training and supporting reference materials to allow them to properly protect the Town’s Information Technology.
- All users must attend an annual computer security workshop given by the designated IT official.
- The designated IT official must develop and maintain a communications process to be able to communicate new computer security program information, security bulletin information, and security items of interest.

Server Hardening: Servers are depended upon to deliver data in a secure, reliable fashion. There must be assurance that data integrity, confidentiality and availability are maintained. One of the required steps to attain this assurance is to ensure that the servers are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service.

The purpose of this policy area is to describe the requirements for installing a new server in a secure fashion and maintaining the security integrity of the server and application software and applies equally all individuals that are responsible for the installation of new IT computer systems, the operations of existing Information Technology, and individuals charged with Information Security.

- A server must not be connected to the Town of Beekman network until it is in a Town IT accredited secure state and the network connection is approved by Town’s designated IT official.
- The Server Hardening Procedure provides the detailed information required to harden a server and must be implemented before use.

Some of the general steps included in the Server Hardening Procedure include:

- ❖ Installing the operating system from an IT approved source
- ❖ Applying vendor supplied patches
- ❖ Removing unnecessary software, system services, and drivers
- ❖ Setting security parameters, file protections and enabling audit logging
- ❖ Disabling or changing the password of default accounts

- The designated IT official will monitor security issues, both internal to the Town and externally, and will manage the release of security patches on behalf of The Town of Beekman
- The designated IT official will test security patches against IT core resources before release where practical.
- The designated IT official may make hardware resources available for testing security patches in the case of special applications.
- The designated IT official is responsible to implement Security patches within a reasonable timeframe after notification from Software Company.

Software Licensing: End-user license agreements are used by software and other information technology companies to protect their valuable intellectual assets and to advise technology users of their rights and responsibilities under intellectual property and other applicable The purpose of this policy area is to establish the rules for licensed software use on Town Information Resources laws and applies equally to all individuals that use any Town Information Resources.

- The Town of Beekman provides a sufficient number of licensed copies of software such that workers can get their work done in an expedient and effective manner. The designated IT official must make appropriate arrangements with the involved vendor(s) for additional licensed copies if and when additional copies are needed in order to conduct official Town business.

- Third party copyrighted information or software, that the Town does not have specific approval to store and/or use, must not be stored on Town systems or networks. The designated IT official will remove such information and software unless the involved users can provide proof of authorization from the rightful owner(s).

- Third party software in the possession of the Town must not be copied unless such copying is consistent with relevant license agreements and prior management approval of such copying has been obtained, or copies are being made for contingency planning purposes.

System Development: The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents, are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents. The purpose of this policy area is to describe the requirements for developing and/or implementing new software in the Town's Information Resources and applies equally to all individuals that use any Town Information Resources.

- The designated IT official is responsible for developing, maintaining, and participating in a System Development Life Cycle (SDLC) for the Town of Beekman system software applications.

- All software applications must have designated Owners and Custodians for the critical information they process. The designated IT official must perform periodic risk assessments of the software to determine whether the controls employed are adequate.

- All applications must have an access control system to restrict who can access the system as well as restrict the privileges available to these users. The designated IT official is the designated access control administrator (who is not a regular User on the system in question) which must be assigned for all applications.

- Where resources permit, there should be a separation between the administration, user access, and test environments. This will ensure that security is rigorously maintained for the application, while the development and test environments can maximize productivity with fewer security restrictions.

- Where these distinctions have been established, development and test staff must not be permitted to have access to production systems. Likewise, all application software testing must utilize sanitized information.
- All application-program-based access paths other than the formal user access paths must be deleted or disabled before software is deployed to users.

Vendor Access: Vendors play an important role in the support of hardware and software management, and operations for customers. Vendors can remotely view, copy and modify data and audit logs, they correct software and operating systems problems, they can monitor and fine tune system performance, they can monitor hardware performance and errors; they can modify environmental systems, and reset alarm thresholds. Setting limits and controls on what can be seen, copied, modified, and controlled by vendors will eliminate or reduce the risk of loss of revenue, liability, loss of trust, and embarrassment to the Town. The purpose of this policy area is to establish the rules for vendor access to Town Information Resources and support services (A/C, UPS, PDU, fire suppression, etc.), vendor responsibilities, and protection of Town information and applies to all individuals that are responsible for the installation of new Information Resources assets, and the operations and maintenance of existing Information Resources and who do or may allow vendor access for maintenance, monitoring and troubleshooting purposes.

- Vendors must comply with all applicable Town policies, practice standards and agreements, including, but not limited to:
    - Town of Beekman Computer Use Policy
    - Town of Beekman Security Policy
    - Town of Beekman Security and Information Breach Notification Policy
    - Software Licensing Policies
- Vendor agreements and contracts must specify:
    - The Town information the vendor should have access to.
    - How Town information is to be protected by the vendor.

  - ❖ Acceptable methods for the return, destruction or disposal of Town information in the vendor's possession at the end of the contract.
  - ❖ The Vendor must only use Town information and Information Resources for the purpose of any agreement entered in to between the Town and vendor.
  - ❖ Any other Town information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others.

- The Town will provide the designated IT official as point of contact for the Vendor. The point of contact will work with the Vendor to make certain the Vendor is in compliance with these policies.
- Each vendor must provide the Town with a list of all employees working on the contract. The list must be updated and provided to Town within 24 hours of staff changes.
- Vendor personnel must report all security incidents directly to the appropriate designated IT official personnel.
- If vendor management is involved in a Town security incident management the responsibilities and details must be specified in the contract.
- Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by the designated IT official.
- All vendor maintenance equipment on the Town network that connects to the outside world via the network, telephone line, or leased line, and all Town vendor accounts will remain disabled except when in use for authorized maintenance.
- Vendor access must be uniquely identifiable and password management must comply with the Town's Password and Admin/Special Access policy areas. Vendor's major work activities must be entered into a log and available to the Town Board upon request. Logs must include, but are not limited to, such events as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.

- Upon departure of a vendor employee from the contract for any reason, the vendor will ensure that all sensitive information is collected and returned to the Town or destroyed within 24 hours.
- Upon termination of contract or at the request of the Town, the vendor will return or destroy all Town information and provide written certification of that return or destruction within 24 hours.
- Upon termination of contract or at the request of the Town the vendor must surrender all Town Identification badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by authorized the Town Board
- Vendors are required to comply with all State and Town auditing requirements, including the auditing of the vendor’s work.
- All software used by the vendor in providing service to the Town must be properly inventoried and licensed.

Virus Protection: The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate.

Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents, are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents. The purpose of this policy area is to describe the requirements for dealing with computer virus, worm and Trojan Horse prevention, detection and cleanup and applies equally to all individuals that use any Town Information Resources.

- All workstations whether connected to the Town network, or standalone, must use the Town approved virus protection software and configuration.
- The virus protection software must not be disabled or bypassed.
- The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.
- The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.

- Each file server attached to the Town network must utilize designated IT official approved virus protection software and setup to detect and clean viruses that may infect file shares.
- Each E-mail gateway must utilize designated IT official approved e-mail virus protection software and must adhere to the Designated IT official rules for the setup and use of this software.
- Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the Help Desk.

VIOLATION NOTICE:

Violation of this policy may result in disciplinary action, which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student.

Additionally, individuals are subject to loss of Town Information Resources access privileges, and to civil and criminal prosecution.

REFERENCES:

National/Federal

Copyright Act of 1976

Foreign Corrupt Practices Act of 1977

Computer Fraud and Abuse Act of 1986

Computer Security Act of 1987

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Gramm-Leach-Bliley Act of 1999

Sarbanes-Oxley Act of 2002

Family Education Rights and Privacy Act of 1974

Oregon Department of Human Resources

Uniform Trade Secrets Act

Payment Card Industry Data Security Standard

San Diego State University

Texas Department of Information Resources

State

New York State Office of Cyber Security

Employee Acknowledgement:

I have read and been informed about the content, requirements, and expectations of the Town of Beekman Security 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 have read the Town of Beekman Security Policy carefully to ensure that I understand the policy before signing this document and will consult with the Town Supervisor if I have any questions.

Please.

Employee Signature: ____

Employee Printed Name: ____

Date: ____

Vendor and/or Consultant Acknowledgement:

I have read and been informed about the content, requirements, and expectations of the Town of Beekman Security 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 have read the Town of Beekman Security Policy carefully to ensure that I understand the policy before signing this document and will consult with the Town Supervisor or Comptroller if I have any questions.

Business Name: ____

Authorized Representative: ____

Date: ____

THIS PAGE LEFT INTENTIONALLY BLANK

Employee Acknowledgement:

I have read and been informed about the content, requirements, and expectations of the Town of Beekman Security 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 have read the Town of Beekman Security Policy carefully to ensure that I understand the policy before signing this document and will consult with the Town Supervisor if I have any questions.

Please.

Employee Signature: _______________________________________

Employee Printed Name: _______________________________________

Date: _______________________________________

Vendor and/or Consultant Acknowledgement:

I have read and been informed about the content, requirements, and expectations of the Town of Beekman Security 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 have read the Town of Beekman Security Policy carefully to ensure that I understand the policy before signing this document and will consult with the Town Supervisor or Comptroller if I have any questions.

Business Name: _______________________________________

Authorized Representative: _______________________________________

Date: _______________________________________