Town of Essex Comprehensive Public Records and Technology Policy

Introduction:
Public records and the use of technology are inextricably linked in our modern age. As such, this policy covers both topics, simultaneously. It is the responsibility of all Town employees to read, understand, and follow this policy. In addition, employees are expected to exercise reasonable judgment in interpreting this policy and in making decisions about Town records and Town technology. Any person with questions regarding the application or meaning of this policy should seek clarification directly from their Department Head. If the Department Head is unclear about how to answer the question, he or she should seek guidance from the Town Administrator. Failure to observe this policy may subject individuals to disciplinary action, up to and including termination of employment.

Accidents do happen and legitimate accidents generally shall not be considered violations. If an employee accidentally violates any aspect of this policy, it is incumbent upon them to report the accidental circumstances to their supervisor or the Town Administrator immediately. An accidental situation that is not reported immediately shall constitute a violation of this policy.

A1. Public Records Management, In General:
All written, digital, photographic, or recorded materials created or received by the Town of Essex (excepting Junk Mail and SPAM, see below) must be considered public records. The Public Records Laws in Massachusetts impose strict standards for the maintenance and management of public records and some records are exempt from public disclosure under certain circumstances. The details in the various laws are very complex and a number of guides have been published by the Secretary of the Commonwealth (www.mass.gov/sec). Employees are encouraged to review these guides to become more familiar with details but such review is not required. What is required is that no decision shall be made and no action shall be taken if the person involved is either not authorized to do so or does not fully understand the correct course of action, taking into account this policy and all rules, regulations, and laws pertaining to a given decision or action.

NO original or sole instance of a public record (whether eligible for disclosure or exempt from disclosure) may ever be deleted or destroyed in any way without the express permission of the State Supervisor of Records. In the Town of Essex, no individual is allowed to delete or destroy original or sole instances of records of any type, regardless of medium, without the State Supervisor's permission AND the permission of the Town Clerk AND the Town Administrator. When in doubt about the ability to delete or destroy original or sole instances of records, DO NOT ACT. Instead, please consult your supervisor and/or the Town Administrator.

- "Junk Mail" (i.e. any mail or letters that are not welcome or solicited and obviously sent in bulk; especially mail of a commercial nature such as advertising circulars, catalogues, form letters, and general marketing materials) is not considered a public record.
- "SPAM" (i.e. unsolicited bulk e-mail, usually advertising or inappropriate material, sent to large numbers of people) is not considered a public record.

- Duplicate copies of original paper records may be destroyed after ensuring that the original records are intact in their usual place of storage. Destruction of copies of paper records or of original paper records that have been approved for disposal as noted above shall proceed in a manner appropriate for the content of the records.
    - Records that may be disclosed to the general public without any type of control or reservation may be disposed of via recycling, shredding, or simple discard.
    - Records that are in whole or in part exempt from public disclosure shall be disposed of ONLY via shredding.

A2. Personal Information:
The Town of Essex shall take the maximum feasible measures reasonably needed to ensure the security, confidentiality and integrity of personal information, as defined in Chapter 93H, maintained by all Town departments (hereafter "personal information"). Each department head or board/commission chair and all Town employees, shall ensure compliance with this policy and with applicable federal and state privacy and information security laws and regulations.

All departments and boards/commissions shall collect the minimum quantity of personal information reasonably needed by practicality and by law to accomplish the legitimate purpose for which the information is collected; to protect the information against unauthorized access, destruction, use, modification, disclosure or loss; to provide access to and disseminate the information only to those persons and entities who reasonably require the information to perform their duties (or as limited by law); and to destroy the information as soon as it is no longer needed or required to be maintained by state or federal record retention requirements (after receiving permission from the State Supervisor of Records to do so). Adequate administrative, technical and physical safeguards, shall be put in place to comply with all federal and state privacy and information security laws and regulations, including but not limited to all applicable rules and regulations issued by the Secretary of State's Supervisor of Public Records under Chapter 93H. Physical security shall include locking any space where records are kept if an employee is not present to monitor access to that space.

Please keep in mind that personal information is typically required to be segregated from other information of a more general nature, secured in a manner more stringent than other information of a more general nature, and withheld from most requestors. The Department Head or board/commission chair for a given department is responsible for knowing the standards that apply to all records in their possession. If unclear, please approach the Town Administrator.

A3. Transport of Paper Records
Original paper records may not be transported to locations beyond official Town of Essex or School District buildings. If original paper records must go beyond this realm, the original records must be copied and the copies, not the originals, shall be transported. The only exception to this rule would be the need to create duplicate copies of an original document that the Town does not have the capability to duplicate in house (such as large-format plans, color reproduction, etc.).

B1. Technology, In General:
Information Technology is defined as:

- Computers (including servers, workstations, laptops and handheld devices)
- Computer-related hardware (including printers, scanners, special devices)
- Software (including networks and the Internet)
- Telephones, Modems & Handheld devices
- Town of Essex Information Technology infrastructure includes all networks, computers, modems, hubs, software and data.

The Information/Technology (IT) Officer for the Town of Essex is the Town Administrator.

The Town of Essex will ensure the security, integrity and performance of all information technology hardware, software, data, and transaction processes on Town property.

B2. Use of Technology:
The acceptable use of information technology is an important concern for all employees and elected and appointed officials of the Town of Essex. Acceptable use rules are as follows:

- All unapproved software and executable programs are strictly prohibited.
- Technology should be used primarily for official Town of Essex purposes related to the conduct of Town government, to accomplish job responsibilities more effectively. Other uses, such as commercial or political use are expressly prohibited.
- Incidental personal use of technology such as Town e-mail is permitted but, like all e-mail generated on Town systems, is subject to monitoring, and must not be inappropriate.
- Employees who use the Internet on personal time can enhance their knowledge of electronic information resources and sharpen information technology skills. By allowing use on personal time, the Town of Essex builds a pool of computer literate employees who can guide and encourage other employees. Personal time includes breaks, lunchtime and the time before and after scheduled work hours. Employees performing job-related use will always have priority over those desiring access to resources for personal use.
- Personal use must not interfere with the town's business needs or operation in any way and must not violate the law or any other aspect of this policy.
    - NOTE: SOCIAL MEDIA SITES AND SERVICES SUCH AS FACEBOOK, TWITTER, AND MYSPACE SHALL NOT BE ACCESSED FROM TOWN-OWNED EQUIPMENT UNLESS THE ACCESS IS FOR OFFICIAL TOWN BUSINESS AND IS APPROVED BY THE EMPLOYEE'S DEPARTMENT HEAD OR APPOINTING AUTHORITY FOR A PUBLIC PURPOSE. ANYTHING POSTED TO ANY SOCIAL

MEDIA SITE FROM TOWN-OWNED EQUIPMENT BY A TOWN EMPLOYEE MUST BE APPROVED BY THE EMPLOYEE'S DEPARTMENT HEAD OR APPOINTING AUTHORITY AND MUST BE FOR A BONA-FIDE PUBLIC PURPOSE.

- Employees are cautioned that inappropriate postings to social media sites on personal time and/or using solely personal devices and accounts may subject the employee to discipline, up to and including termination, if the postings adversely effect the Town or the workplace. By way of example, and not by way of limitation, inappropriate personal postings that may subject an employee to discipline include threats of violence, comments suggesting that the employee harbors any animosity or bias towards any protected class of individuals or any individual member of a protected class, and the disclosure of personal information or other confidential information gleaned in the workplace.

- Examples of job-related use of the Internet/intranet include: accessing external databases and files to obtain reference information or conduct research; corresponding with the Town's customers and other town employees; disseminating documents to individuals or groups; and participating in discussion groups on job-related topics.
- Inappropriate use of technology includes any activity that is illegal, such as the creation or distribution of pornography, and activities such as political lobbying, or personal or business use to benefit those other than the Town of Essex government. Examples of inappropriate use include, but are not limited to:
    - Activities that could cause congestion or disruption of the network, including downloading and installation of executable programs on the network.
    - Use of abusive or objectionable language in either public or private messages. The telecommunications systems should not be used to create any offensive or disruptive messages or images.
    - Engaging in computer gaming or gambling.
    - Accessing material or sites that contain unlawful or sexually explicit material.
    - Misrepresentation of oneself or the Town of Essex.
    - Lobbying Town Boards or elected officials to advocate for personal or extra-departmental issues.
    - Sending chain letters.
    - Using official dissemination tools to distribute personal information.

<u>B3. Public Nature of Technology/NO EXPECTATION OF PRIVACY</u>

- The Town reserves the right to retrieve, read, and/or analyze any electronic communication messages or any other data stored, created, received, or transmitted on Town-owned equipment.
- All data existing within the Town of Essex Information Technology infrastructure is considered property of the Town of Essex and no assumption of privacy may be made. Employees and other users of the Town of Essex Information Technology

infrastructure should have NO EXPECTATION OF PRIVACY with respect to their communications or other use of the technology.

- E-mail does not have the same privacy safeguards afforded regular mail or telephone communications. A good standard to apply is: Do not send an e-mail you would not want printed on the front page of the local newspaper.

B4. Operational Requirements of Technology

- Users are required to maintain the privacy of passwords and are prohibited from publishing or discussing passwords with others (except with the IT Officer or his designee).
- Should a user suspect that their password or access has been observed or compromised, the user shall immediately change their password or request assistance in doing so from the IT Officer.
- Users are forbidden from attempting to access files that are held in the realm of other users' or other departments' secure file spaces (unless they have been officially granted shared rights). Although system security should not allow this type of access to occur, if it unintentionally does occur, the user should immediately report the issue to their department head and/or the IT Officer. Any user found intentionally attempting to break into areas that they do not have rightful access to or found intentionally perusing or otherwise consuming information in such areas shall be deemed to have violated this policy.
- In order to maintain compliance to licensing and copyright law, and to increase security and reliability of systems, software installation is allowed only within the following parameters:
    - The software is licensed to the Town of Essex.
    - The person installing the software is expressly authorized to do so by the IT Officer.
- In order to maintain a secure, stable and operational network, hardware and peripheral installation is allowed only within the following parameters:
    - The equipment is owned by the Town of Essex and has been inventoried and accepted for use by the IT Officer.
    - The person installing the equipment is expressly authorized to do so by the IT Officer.
- Since all data within the Town of Essex Information Technology infrastructure is subject to monitoring and is considered public information, attaching personal equipment (such as laptops, or flash drives) to the Town of Essex IT Infrastructure is not permitted without the express authorization of the IT Officer.
- Computer users are expected to use hardware and software in a manner that enables its ongoing usage. If a piece of equipment malfunctions, the user is to notify the IT Officer in a timely manner so that the equipment may be assessed for damage and replaced or repaired. No equipment or software is to be disposed of by anyone but the IT Officer.
- All data received from sources outside the Town of Essex including the Internet, floppy disk, zip disks, USB drives and tape are to be scanned for viruses. If any source is questionable, the IT Officer should be consulted prior to downloading or uploading data to Town of Essex computers.

- The IT Officer shall back up all Town data regularly and shall include off-site and disaster recovery strategies as outline in the Town's Continuity of Operations Plan.
- The IT Officer has implemented a procedure that copies ALL incoming and all Town domain (essexma.org) outgoing e-mail to a central storage area. Incoming traffic includes ALL traffic generated from ANY e-mail account on ANY type of device, including handheld devices, even if such device is personally-owned – since incoming traffic to the Town is all sent to official, essexma.org e-mail accounts.
- Even though a backup copy may be available, no computer user is authorized to permanently delete ANY e-mail (either incoming or outgoing) from their workstation unless the e-mail in question is clearly incoming SPAM (i.e. unsolicited bulk e-mail, usually advertising or inappropriate material, sent to large numbers of people); or the incoming e-mail in question is clearly incoming "Junk Mail" (i.e. any mail or letters that are not welcome or solicited and obviously sent in bulk; especially mail of a commercial nature such as advertising circulars, catalogues, form letters, and general marketing materials); or the incoming e-mail in question is likely or actually infected with a virus. It is not envisioned that records of outgoing e-mail would ever have a valid reason for deletion and no user shall intentionally configure the e-mail system on a Town computer or account so that copies and/or backup copies of sent messages are not generated.
- E-mails may be organized into logical folders within a user's e-mail system and may be moved from the user's "inbox" via the "delete" key or icon so long as the e-mail system places the message(s) in a "deleted items" or other appropriate folder (i.e. the message is just moving to another folder and not actually being deleted from the system).
- All procurement of Information Technology (as defined above) shall be made through the IT Officer, or with his permission.
- Employees must have written permission from the IT Officer to remove from Town offices Town-owned technological devices of any kind and must sign a statement identifying all of the equipment in question and indicating that they are responsible for the well-being of the equipment and the safeguarding of any data stored thereupon.
- All computer repairs will be made on Town property, with limited exceptions, to ensure that confidential data has adequate controls.
- Employees are permitted to monitor Town e-mail using personal devices. However, for those employees who have a Town-issued, Town-owned computer in the work environment, all such activity must ensure that copies of incoming e-mail are kept on the Town's hosted e-mail server until it can be downloaded using the employee's Town-issued equipment that exists in the work environment the next time they access their e-mail at work. Employees shall also ensure that personal information is safeguarded on their personal devices if the source of that information is the Town's e-mail system or IT infrastructure. Further, all provisions of the Public Records Law and this policy apply as well to personal devices used to transmit, receive, create, or store information for public purposes.

B5. Specific Security Policies and Procedures

Password Management:
The Domain controller shall be set to the following policies:

Enforce Password History	6 Password Remembered
Maximum Password Age	90 Days
Minimum Password Age	10 Days
Minimum Password Length	8 Characters
Password Must Meet Complexity Req.	Enabled
Account Lockout Duration	60 Minutes
Account Lockout Threshold	4 Invalid Attempts
Reset Account Lockout Counter After	60 Minutes

Users only have domain accounts and do not log onto local desktops on PCs. Everything is virtualized.

Incident Response:
In the case of a virus or crypto attack, the Town Administrator will log out the user and contacts personnel from Danvers IT. Those personnel help segregate the problem and clear the issue.

In the case of a potential breach of protected information (not public records), the Town Administrator will contact Town Counsel and the Town's insurer for careful consideration of the matter, including the development of a plan for all necessary public outreach and any benefits to be extended (such as credit monitoring). Further, Town Counsel will draft for the Town any and all required disclosures.

Data Management:
All data, including Windows desktop settings for each user, is mirrored to a second live instance of the production environment that is resident at the Danvers datacenter backup site (Danvers provides the primary live instance from its datacenter for direct computing over a dedicated fiber link as well). Also, all user-created files that are stored on the central, virtual file server are backed up separately to Carbonite each evening.

Physical Access:
The IT infrastructure in Essex is very centralized, with all users' Windows desktops residing on virtual servers running on hardware at the Danvers datacenter (all Town buildings are connected to Town Hall and each other via direct, municipally-owned fiber – Town Hall connects to Danvers via a dedicated, municipally-owned fiber link). ONLY the Town Administrator (who serves as the IT Officer) has a key to the server room. The master key to Town Hall operates all locks, except for the server room. The Town Administrator does keep a backup key in his office that the Selectmen's Assistant may have access to, with

permission from the Town Administrator on a case-by-case basis. This key may be used when something needs to be checked on or an authorized vendor or consultant needs access and the Town Administrator is not available (or in some type of emergency).

Physical access to routers and switchgear in individual buildings is limited due to the locations of this equipment. Individual department heads in remote buildings (i.e. not Town Hall) contact the Town Administrator if anything seems amiss with this remote equipment.

Change Management:
The Town of Essex seeks to prepare, equip, and support all IT users with respect to each new change that occurs within the Town's IT infrastructure, software suite, and Windows desktop environment. Generally, the Town Administrator plans all changes with appropriate consultants and personnel from the Town of Danvers IT Department (which hosts the Town's real-time backup system). Subsequently, he works with each user to explain the change and to arrange for any appropriate training. As the change occurs, the Town Administrator is in contact with each user, monitoring the expected result and answering questions. If corrections are needed for any user, the Town Administrator makes all necessary adjustments.

Vendor Management:
The Town's slate of usual vendors is very static and each vendor provides ongoing support directly to each department using an application. The major vendors are City Hall Systems, Vadar Systems, Patriot Properties, OpenGov, Harpers, Microsoft (for Office 365 and e-mail), the North Shore 911 Emergency Dispatch Center, the State Criminal Justice Information System, NetTelOne (VOIP telephone vendor), Weston & Sampson (sewer SCADA vendor), the State voting system, and the Merrimack Valley Library Consortium. Most often, vendor support is managed entirely by each department and the Town Administrator becomes involved only with respect to hardware or server access. The Town of Danvers IT Department provides direct computing via remote virtual servers, the Town's real-time backup system, and a Regional Security Fabric on the Fortinet Platform as part of the North Shore IT Collaborative.

Approval and Documentation of Changes:
Should a department require a change, the Town Administrator makes the change and documents new settings. Should the Town Administrator need to make a change more globally, without departmental request, the change is documented internally and at Danvers IT. In addition, major changes of this nature are discussed with the Board of Selectmen at public meetings.

Training
Annually, the North Shore IT Collaborative will provide network penetration testing and user phishing and social engineering testing. Further, each user must

annually review and acknowledge the Town of Essex Comprehensive Public Records and Technology Policy.

B6. Asset Management and Disposal

Procurement of IT Assets:
If a given department is in need of an IT-related asset that requires joining with the Town's local area network, the department head contacts the Town Administrator concerning the required specifications. The department may then order the asset and the Town Administrator configures the asset once it has been received. The Town Administrator retains the local machine administrative password, which is not shared with the department.

Other IT assets that are not part of the Town's local area network also exist but these are managed by outside partners such as the North Shore 911 Emergency Dispatch Center, the State Criminal Justice Information System, NetTelOne (VOIP telephone vendor), Weston & Sampson (sewer SCADA vendor), State voting system, Merrimack Valley Library Consortium, Patriot Properties, Vadar Systems, Harpers, City Hall Systems, OpenGov, Microsoft and the Town of Danvers IT Department.

Management of IT Assets:
The Town Administrator directly manages all assets that are part of the Town's local area network. If an asset needs maintenance, repair, or updating, the Town Administrator takes those actions.

Other IT assets are managed by outside partners.

Disposal of IT Assets:
When any asset owned by the Town is disposed of, all hard drives are removed and the chassis is recycled. Hard drives are physically destroyed by passing a power drill through each drive at least seven times and then recycled.

C1. Special Provisions, In General
Certain employees will be involved with transactions and activities that carry specialized requirements and protocols for the management and security of information. These are outlined below.

C2. Criminal Offender Record Information (CORI)
Any employee who seeks CORI must be specifically authorized by the Department of Criminal Justice Information Services (CJIS) to do so. In seeking such authorization, each employee will receive training and guidance from CJIS as to the narrow focus of their authorization, protocols that must be followed, and CORI security and destruction. It is important to note that even the destruction of CORI documents must be approved by the Massachusetts Supervisor of Records before proceeding. Any CORI-certified employee is expected to follow all rules and guidance issued by CJIS relative to their

specific certification and is expected to follow the Town's CORI Policy. Presently, only the Town Administrator and the Chief of Police and his designees are authorized to receive and manage CORI. Any employee interested in becoming so-authorized must be able to substantiate a specific reason to CJIS and must obtain the permission of the Town Administrator in advance.

C3. Personnel Records

The Town of Essex Personnel Rules & Regulations require that each Department Head provide a copy of any paper personnel-related document to the Personnel Officer (Town Administrator). Departments Heads should be sure to follow this practice.

C4. Health/Medical Records and HIPAA

Town Departments, officials and employees that have specifically been designated as health care components in the Town's Designation of HIPAA Hybrid Entity Status are required to comply with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"). These designated Town Departments, officials and employees should refer to the Town's HIPAA Privacy and Security Policies to ensure compliance with HIPAA's confidentiality provisions. Absent narrow exemptions, health and medical information pertaining to individuals is confidential, and thus, exempt from public disclosure under HIPAA and state law.

Examples of confidential medical information may include physicians' notes for extended periods of illness, physicians' return to work clearances, applications and results regarding pre-employment drug/medical screens, DOT commercial driver's license drug screens, etc. When in doubt, any employee charged with managing such records should treat such information as confidential by keeping it in a separate, medical folder, in a separate, secure file area where all such folders are stored. All employees should refer, as necessary, to the Town's "Notice of Privacy Practices" to ensure that all necessary steps are being taken with regard to individuals' confidential medical information. If there are any questions related to the confidentiality of health or medical information, inquiries should be brought to the attention of the Town Administrator, who serves as the Town's HIPAA Privacy Official.

Town of Essex Comprehensive Public Records and Technology Policy

EMPLOYEE ACKNOWLEDGMENT:

I have read and understand this policy. If questions arise in the future, I will consult my supervisor and/or the Town Administrator before taking action regarding the topics covered herein.

_____ _____

Printed Name Date

_____

Signature