Table of Contents

Section 1: Introduction

Reducing the cost of operations, improving productivity, and enhancing services to its constituents should be the goals of every local government. The Town of Batavia achieves these goals through use of a enterprise content management system (ECMS). The town's ECMS will increase access to various records stored on the system. Increased access to records in the system will allow town employees to improve services to town residents.

The town's ECMS is a large database program with various unique functions used to create, modify, route, store, retrieve and distribute the town's electronic records in the system.

The town's new system comes with a records management application (RMA) designed to track the correct records retention requirement for each electronic record in the system in accord with the New York State Archives "Record Retention and Disposition Schedule MU-1, For use by Cities, Towns, Villages, Fire Districts" issued in 2003.

This procedures manual was developed by the town's Technology and Records Management Committee in consultation with James M. Tammaro from the New York State Archives and is based, in part, on various New York State Archives publications and training materials.

The Committee's mission is to provide the necessary administrative support for formulating and implementing a legally compliant ECMS in town government. Members of the Committee include: the town supervisor, the deputy town supervisor, the town clerk who also serves as the town's records management officer (RMO) and the town assessor.

Responsibilities of the committee include: (1) ensuring good lines of communication between town officials and department heads in town government, (2) addressing various records management requirements associated with the electronic records placed in the ECMS, (3) identifying appropriate electronic records management projects and strategies for the town's ECMS, (4) reviewing new request for proposals (RFPs) and developing responses to RFPs for new activities associated with the town's ECMS, (5) developing and periodically reviewing electronic records plans, policies and procedures and (6) ensuring ongoing staff training on the ECMS.

The goals of this manual are to ensure:

- The Town of Batavia operates and manages the town's new ECMS in a consistent manner,
- The electronic records managed by the system are easily accessible,
- The electronic records in the system are preserved for their legal retention period and
- The electronic records produced by the system are legally acceptable.

Copies of the manual will be provided to each town employee creating and using the electronic records in the ECMS. The manual will be updated on a regular basis as additional town records are added to the system and as technological updates to the ECMS occur.

For additional information about the town's ECMS and/or the electronic records managed by the system, contact Teressa Morasco, the Batavia Town Clerk. Ms. Morasco can be contacted by phone at: 585.343.1729, ext. 203 or by e-mail at: tmorasco@townofbatavia.com.

Section 2: Guidelines for Using this Manual

This manual is organized by various topics relating to accessing, managing, preserving and retaining for their legal retention period the electronic records in the ECMS and adding additional records to the system.

The Batavia Town Board determined all town employees given the authority to use the town's ECMS to manage electronic records on the system must consult this manual on a regular basis to ensure the electronic records placed in the system are managed in a consistent manner throughout town government.

Therefore, any new town employees or employees who have not used the ECMS in the past must read this manual before uploading or using the electronic records placed in the ECMS.

Users of the manual are encouraged to consult the table of contents at the beginning of the manual as a means for gaining quick access to the information they are looking for in the manual.

The Town of Batavia will update this manual on a regular basis to reflect changes in the types of electronic records stored on the ECMS, the practices for managing the electronic records stored on the ECMS and/or the changes in various technologies associated with the ECMS. Therefore, if any employees have suggestions for making changes to the manual, those suggestions should be directed to the Batavia Town Clerk and RMO. Any questions or concerns regarding the use of this manual and/or the ECMS should also be directed to the town's RMO.

Please note, in addition to using this manual for operation and maintenance of the town's ECMS, staff should also consult the town's general technology policies and the Town of Batavia Employee Policy Handbook.

Section 3: The Electronic Records Filing Plan

Establishing and adhering to a good electronic records filing plan is essential to maintain the electronic records created in the town's new ECMS. Therefore, it is important for all employees creating, using and maintaining electronic records in the town's ECMS to follow the automated filing plan already established for the electronic records in the ECMS which has been programmed into the system.

Therefore, it is important for employees managing the electronic records cited below, which are stored in the ECMS, to follow the filing system already programmed into the ECMS. It is especially vital to follow the default filing plan for those electronic records which are meant to be shared across town government offices.

A good electronic filing plan utilizes a controlled vocabulary for:

- The names of electronic folders holding the records,
- Index terms used to locate the electronic records
- The electronic filing plan itself

The plan should also control the access rights to various electronic records.

The electronic filing plan designed for the town's ECMS is based on the business needs of the departments filing electronic records in the ECMS in terms of need and access to the electronic records. The filing plan is simple, logical and uses only a few hierarchical levels in the already established filing structure. In addition, the titles of folders, sub-folders and files were kept simple, clear and consistent. This should help ensure the new ECMS will be easy to use and maintain.

The filing plan is based on the organization of various departments using the system and the primary functions of those departments. In addition, where possible, the file plan is designed to encourage filing records with the same or similar records retentions together.

The filing plan was modeled on the existing filing plan for the paper versions of the electronic records in the ECMS. The plan is designed to be a consistent method for filing the electronic records in the system and incorporate how town employees and other individuals who would have access to the system would search for records on the system.

The initial filing plan for using the ECMS was designed for filing, on the ECMS, the following electronic records: (1) town board meeting minutes, (2) building permit files, (3) property record cards, and (4) deeds for properties. Below is a graphical illustration depicting which drives, folders, sub-folders should be used for filing the above electronic records on the ECMS.

Graphic illustration of electronic file classification scheme on the town's server to be inserted here by the town.

Section 4: Training

When creating, using, maintaining and preserving the electronic records placed on the town's new ECMS, it is important to ensure the authenticity and legality of those records for various reasons. Having employees who are using the electronic records placed on the ECMS properly trained is crucial to ensuring the authenticity, legality and confidentiality of the records placed on the system.

Therefore, town officials have determined that before using the ECMS, employees must be properly trained on all aspects of the system.

In addition, anytime the system is upgraded with new software, hardware or a revised filing plan, all employees must once again participate in some form of training to familiarize themselves with the changes in the ECMS.

All staff using the ECMS must be trained on how to access and manage the electronic records stored on the town's ECMS but also on all of the town's electronic records policies.

Section 5: Security Issues

Electronic records placed on the town's ECMS are subject to various security threats just as paper records would be. Therefore, generally speaking, the Town of Batavia has taken some comprehensive measures to increase the security for the town's electronic records by placing fire detectors in the areas where the computer equipment is housed and have incorporated the electronic records into the town's disaster recovery program.

However, there are a number of security measures town employees should take, on an individual basis, to increase security for the electronic records placed on the town's ECMS. It's very important for town employees using the records stored on the town's ECMS to adhere to these security measures to increase the security for the electronic records placed on the system.

These security measures can be categorized as physical security measures and technical security measures.

In terms of the **physical security measures**, employees should make sure the doors are locked to any room where the computer equipment used to gain access to the town's electronic records is placed.

In addition, employees must not allow the public to use their computer to access the electronic records in the ECMS but, must instruct the public to use the public access terminal established for public access to the electronic records in the ECMS. For example, if an employees computer equipment resides in a room used for public meetings in the evening, employees should make sure their equipment is turned off so no access by the public is possible with the employee's computer.

Still another very important measure is for town employees to make sure their computer has automatically logged them off the system when their computer is going to be left unattended so there is no unauthorized access to the employee's computer and unauthorized access to the electronic records in the ECMS.

In terms of the **technical security measures**, the goal here should be to reduce the technical or electronic risks to the records.

One activity related to this topic is to avoid any software from unknown sources. In fact, town employees must not install or run software other than the software approved for use on the town's network. Employees should be particularly wary of any software sent as e-mail attachments or files with executable programs as these files can carry a virus which can infect the security of the ECMS and the security of the electronic records placed in the ECMS.

Using passwords and changing their password every 30 days is another fairly simple activity which employees must use in connection with using the electronic records placed in the town's ECMS. The use of passwords protects the electronic records placed on the town's ECMS because they restrict access to the electronic records to authorized individuals and because they can protect the records from unauthorized changes to the electronic records.

Employees must use passwords to gain access to their computer, their e-mail account and to gain access to the electronic records in the ECMS which are designed to be only accessible by employees within that department.

When creating a password, town employees are advised that the password must contain seven characters, including at least one of each uppercase, lowercase letters and number and/or special character. When employees are changing their password, the new password must be substantially different from the old password and should not be a common name or word.

Another simple activity town employees can take to increase security for the electronic records placed on the town's ECMS is to routinely back-up the records placed on the system.

It should be noted that making back-ups of electronic records placed on the town's system are designed as a disaster-recovery measure and not intended for long-term storage as a preservation alternative. Therefore, the back-ups to the electronic records must be stored a substantial distance from the town offices where the ECMS is being used.

In order to increase security for the town's electronic records placed on the ECMS, town employees must adhere strictly to the back-up procedures.

When backing up the records, the appropriate retention period must be applied to the electronic records on the back-up media so when the retention period for those records has been met, the town will not only delete the copy of those electronic records on the server containing the ECMS but, also on any copies of the records placed on back-up media.

In keeping with the above thought, town employees must back-up the electronic records according to the following schedule:

<u>Town board meeting minutes</u>: back-up each night onto an external hard drive with the external hard drive being changed out weekly and the back-up being stored in a place to be determined.

<u>Building permit files</u>: back-up each night onto external hard drive, with the external hard drive being changed out weekly and the back-up being stored in a place to be determined.

<u>Property record cards</u>: back-up each night onto external hard drive, with the external hard drive being changed out weekly and the back-up being stored in a place to be determined

<u>Deeds to properties</u>: back-up each night onto external hard drive, with the external hard drive being changed out weekly and the back-up being stored in a place to be determined

Section 6: Providing Access to Records in the System

For the purpose of this manual, providing access to the electronic records in the town's ECMS means giving someone the permission, opportunity and ability to use the electronic records stored in the town's ECMS.

Before giving someone permission to use the records in the system, the person primarily responsible for managing a certain group of records in the system must assess all the confidentiality, privacy and security issues associated with the group of records before determining it is appropriate to allow access.

Providing opportunity to use the electronic records in the system involves making it possible for individuals to view records directly in person or through a surrogate (photocopy or digital image, for example)

In order for individuals to use a record in the system, the record must be in a format that is readable either directly or with the necessary software and hardware associated with the town's ECMS. The intended use of the records may determine the format in which you provide access to the records. Also, obviously, the format of the records can determine the types of equipment you need to provide access (photocopier, hardware, software, etc.)

When analyzing the confidentiality issues associated with giving access to certain electronic records in the system, staff should analyze the level of confidentiality so if records contain private information about individuals (social security numbers, home addresses, phone numbers, etc.) it may mean staff will provide information about the records without providing direct access to the record or staff will provide a copy of the record with certain information redacted from the original electronic record due to reasons of confidentiality.

In keeping with the above, if the town determines it should use the redaction function on the ECMS, the town's official policy for when information is redacted must be strictly adhered to in a consistent manner.

In many cases, public access to the electronic records in the system will be through the designated public access terminal in town hall.

Physical access to the records in the system will be governed by the following policies:

1. Reference policies – See appendix #1 for the town's reference policies document for staff who are providing access to the electronic records in the system.
2. Rules for use policy – See the appendix #2 for the town's policies for individuals wishing to use the electronic records in the town's ECMS.
3. New York's Freedom of Information Law – New York's Freedom of Information Law (FOIL) requires the appointment of a records access officer to coordinate the town's response to the public's request under the FOIL law. The records access officer for the Town of Batavia is Teressa Morasco, the town clerk and RMO. Therefore, when staff are presented with a FOIL request for electronic records on the system, staff should contact Teressa to obtain further guidance on responding to the request. See appendix #3 for additional information about New York's FOIL Law.

Finally, in terms of access, it should be noted that if the town is faced with a warrant for records, compliance must be immediate. The town can require two forms of ID to verify the requestor's identity and this matter should be discussed with the town attorney.

Section 7: Internal Audit Trails and Access Logs

The town's use of an audit trail is an excellent method for proving the reliability of the town's ECMS. The auditing activities will allow the town to: (a) monitor and detect who had access to the town's ECMS, (b) whether staff followed the rules set out in this manual and (c) any fraud or unauthorized acts which occurred relative to the system.

The town can track AppXtender Audit Trail. AppXtender Audit Trail allows the town to track user activities such as user login/logout, viewing and deletion of documents and pages, addition and deletion of annotations, batch indexing, printing and queries, and annual routine check of audit trails.

The events to be audited are configured through AppXtender Application Generator (AppXtender, AppGen) and can be enabled or disabled for an application, user or group. When user activity triggers an audit event, details of the event are recorded in the audit trail. Each line in the audit trail represents a single audit event. Depending on the configuration, the audit trail can contain status information for each application and global audit events.

AppXtender Desktop and Web audit trail logs cannot be separated. If Audit Trail is enabled and AppXtender Web is installed, both AppXtender Web and AppXtender Desktop events will be tracked.

After audit settings are configured, the town can choose to store audit trail events in the AppXtender audit trail database table or in a log file or both. Application Xtender Audit Trail encodes the time column *tsstamp* in the AE_AUDIT table in Greenwich Mean Time (GMT) format. This allows the audit table entries to maintain consistency when workstations are located in multiple time zones. The town can calculate its local time by supplying the town's time zone to offset.

The following AppXtender Web activities can be tracked using Audit Trail:

- Modification (including annotations) of documents.
- Modification of document indexes
- Viewing of document pages
- Printing of documents and pages
- Addition, deletion, annotation, OCR/Text-view of a page version
- Batch indexing
- Adding, deleting, or attaching pages to a batch document
- Deleting or adding memos to batches
- Executing queries
- User login and logout of the AppXtender Web system

In summary the audit trail capability allows tracking of user activities on a global or per-application basis. Audit events, such as the creation, changes, or deletion of documents can be tracked for each AppXtender application. There is no reporting audit in Application Extender. By default, AppXtender logs audit trail events to a table in the AppXtender database, which can be accessed through the database software.

Anytime a record is added, modified or deleted, a record is created in a database table to audit the changes. The Application Xtender audit table can be accessed from the server.

The town will routinely check the audit trails and the access logs for the ECMS as part of its routine maintenance procedures for the ECMS.

Section 8: Records Creation Issues

A crucial aspect of ensuring the authenticity and reliability and access to the electronic records placed in the town's ECMS relate to how the electronic records placed in the system are created.

When creating electronic records in the system, staff must follow the procedures described below:

1. **Document preparation** – The paper records scanned into the ECMS must first be properly prepared for scanning. Document preparation will include collating the paper records, removing any fasteners attached to the paper records such as staples, paper clips, pins, rubber bands and, if necessary, flattening, unfolding or unrolling the records. This activity will be carried out by the town department responsible for creating the record as part of that department's normal operations.
2. I**mage capture** – The next step will be to scan the paper records to be entered into the ECMS. The speed at which the paper records can be scanned can vary due to a number of factors however, generally speaking, it should be possible to scan the paper records at a rate which is approximately ½ of the rated capacity for the town's scanner.

   Before scanning the records, it will be necessary to determine the block-out color for the scanner which is the color the scanner will not pick up when the paper records are scanned. Obviously it is important the records being scanned do not contain any information in the same color as the scanner's block-out color as that information would not appear on the digital image of the paper records being scanned.

When scanning the paper records, the town must adhere to the New York State Archives Imaging Production Guidelines which appear as appendix #4. Among other things, these guidelines stipulate the official copy of a digital image of a paper record must be in the TIFF format therefore, all official copies of digital images of records stored in the town's ECMS must be in the TIFF format.

This activity will be carried out by staff in the town clerk's office. After scanning the paper records, staff in the office will verify the content of the scanned image of the record to make sure every image is legible and all documents were properly scanned.

3. **Indexing the Electronic Records** - After the paper copy of the records are scanned and the digital images of the documents have been verified, the digital images must be indexed for ease of retrieval. The digital images of records in the building permit files must be indexed by permit number, the digital images of the property record cards must be indexed by SBL # and the digital images of the deeds to be entered into the ECMS must be indexed by SBL #. The town has determined the official copy of the town board meeting minutes will be stored in the PDF format in addition to the TIFF format to allow for full-text searching of the digital images of the minutes, using the proper software.

   Staff from the town clerk's office will carry out this activity.

4. **Filing the electronic records** – After the digital images of the scanned records have been properly indexed, the electronic records must be filed according to the automated filing system programmed into the ECMS.

Section 9: Records Retention Matters

Printing out any of the electronic records placed in the ECMS and considering the paper copy of the record as the official copy of the record is one option for meeting the official retention period for the electronic records in the system in accord with the New York State Archives “Records Retention and Disposition Schedule MU-1 for Use by Cities, Towns, Villages and Fire Districts”. However, that is a costly and inefficient method for adhering to the retention period for the electronic records in the ECMS.

In most cases, a better option is to use the electronic format of the records in the ECMS to meet the legal retention period for those records. In order to do this effectively, employees must determine the legal retention period for any electronic records placed in the ECMS when the electronic records are added to the ECMS. Therefore, employees are strongly urged to utilize the RMA which is part of the ECMS to “label” or “attach” the appropriate retention period for the electronic records when they are entered into the ECMS. Employees should work with the town’s IT person to develop a strategy for routinely attaching the appropriate retention period for any electronic records added to the system.

The above activity may be accomplished at the records series level (a records series is a group of records which all have the same function) such as attaching the same retention period for property record cards which would be one records series which would all have the same retention period.

No matter what strategy an employee uses to associate the appropriate retention period with the town records in the ECMS, that strategy must be documented in writing and be consistent since the focus in recent court rulings regarding electronic records has been the retention and disposition of the electronic records.

Section 10: Dealing with Legal Issues

To effectively deal with legal issues relating to the electronic records in the town's ECMS, it is important to understand the current legal framework for electronic records.

The legal framework discussed in this section includes: (1) State Law, (2) Court Cases and (3) Federal Rules of Civil Procedure.

State Law – In New York State, the State's Arts and Cultural Affairs Law defines records as existing in any media thus establishing electronic records as being subject to the same requirements as paper records or records on microfilm.

In addition, the New York State Education Commissioner's regulations provides details on how to comply with the Arts and Cultural Affairs Law and charges governments, such as the Town of Batavia, with including records retention issues and instituting other records requirements into the design of any electronic system to ensure the electronic records are accessible for the entire legal retention period. That system design must involve the creation and maintenance of metadata, the distribution of back-up copies of electronic records and taking the necessary measures to ensure media integrity.

Further, the 2006 amendments to New York's Freedom of Information Law (FOIL) require local governments to respond to FOIL requests by e-mail if they have the ability to do so and supply the requested records in electronic form if they have the ability to do that also.

Further, FOIL does not distinguish between electronic records created at a work place or on a computer outside of the workplace as government records are open to FOIL requests regardless of where they reside.

Court Cases – Some high-profile court cases have established the value of electronic records and have established that electronic records are vulnerable to legal discovery actions. Further, recent court cases regarding electronic records have emphasized the importance of using appropriate records retention schedule requirements for the electronic records in an organization and have stressed appropriate behavior when those electronic records are the focus of a court order.

Federal Rules of Civil Procedure – The most significant federal legislation pertaining to records consists of recent amendments to the Federal Rules of Civil Procedures (FRCP) which were enacted in December of 2006.

Initially, these amendments applied only to electronic records relevant in federal cases however, they have already been adopted by several states and they bring new prominence to existing state legislation and regulations pertaining to electronic records.

The amendments also provide a "safe harbor" regarding electronic records which is intended to place a limit on the extent of effort a defendant must expend to locate or produce electronic records, provided the defendant can demonstrate the records are inaccessible in spite of all best efforts.

In view of the above, it is very important the town be knowledgeable about exactly what electronic records are stored in the town's ECMS since under the new Rules, both parties are required to meet within 90-120 days of an e-discovery action to review a list of potentially relevant records.

Also, to prove the town regularly disposes of the electronic records placed in the ECMS, according to the MU-1 records schedule and according to the town's official policies and procedures, the existence of written polices and procedures is crucial in order for the town to make a good case it is claiming a "safe harbor".

Finally, regular staff training on how to use the town's ECMS will also be crucial to responding to legal matters regarding the town's electronic records placed on the system because the control of said electronic records in the town's ECMS depends on the individual user of the ECMS.

When town employees are asked to testify in court regarding the electronic records in the town's ECMS, individuals must be prepared to explain the recordkeeping practices associated with the ECMS including why, how, by whom, and when the electronic records were created using the ECMS and how they are maintained, accessed, and migrated.

In addition, staff should be prepared to identify potential causes of error including assessing the probability of errors creeping into records during creation, maintenance, access and migration.

Also, staff should be able to explain the security strategies in place with the ECMS and show steps which were taken to prevent errors and breaches and the procedures in place for updating the security of the system.

Further, staff testifying in court should be able to document the staff training which has occurred in an effort to demonstrate that staff know how to use the system and that they follow procedures for using the records stored on the system.

Finally, employees testifying in court should be prepared to prove the electronic records which were destroyed from the ECMS were destroyed in accord with the New York State Archives "Records Retention and Disposition Schedule MU-1 for Use by Cities, Towns, Villages and Fire Districts" to dispel any concerns about the legality of the disposition. Individuals should be able to demonstrate the town used a records disposal form to document the disposal of the electronic records which have met their legal retention period and a purging log was maintained.

System Documentation: EMC ApplicationXtender electronically stores, organizes, and manages documents, files and other business-critical information, and provides fast, security-controlled access to information from Microsoft Windows or Web-based clients. Application Xtender integrates document imaging, reports management such as Computer Output to Laswer Disc (COLD), and Enterprise Reports Management (ERM), workflow, and document management services within an easy-to-use Windows system.

ApplicationXtender release 6.0 expands its supported retention management offering by adding ApplicationXtender Software Retention Management (SRM). SRM is a licensed component that provides a software solution for document retention management within ApplicationXtender. Documents filed for retention cannot be modified or deleted from the repository until the specified retention period expires. Retention is enforced at a file level by ApplicationXtender's secure path feature. A related enhancement includes the ability to create SRM- and Center-enabled applications using the ApplicationXtender Migration Wizard.

Minimum hardware requirements –

- Processor: Server-class PC (Multiple processors are supported).
- Available hard disk space: The K2 software is approximately 2 GB. The additional space take up by the collections will be approximately 40% of the aggregate size of the documents indexed.
- Memory: Recommended – 1 GB or RAM

- Processor: Minimum – Pentium 4, 2 GHZ (or the minimum CPU required to run the operating system, whichever is higher). Recommended – Pentium 4 HT, 3 GHZ or higher. Dual or quad processors recommended for high-volume deployments.
- Available hard disk space – Depending on the operating system, installation requires approximately:
    - 109 MB (for Application Xtender Rendering Server and Component Registration.
    - 109 MB (for Application Xtender Web Services, Component Registration, Web Services Test Client, Web Services Client Code Samples and Web Services Text Utility).
    - 170 MB (for Application Xtender Utility Services and Component Registration).
    - The ApplicationXtender File Access Manager Server requires a minimum of 1GB free space on the system partition. (Recommended – 2 GB)
- Speed - Fast SCSI hard drives with access times less than 0.5 ms are recommended for best performance.
- Memory – Recommended – 1 GB of RAM.

For the ApplicationXtender Distribution Extraction Workstation

- Processor – Pentium 4 (faster processor increases ApplicationXtender Distribution Productivity)

- Available hard disk space – The ApplicationXtender Distribution Extraction software requires about 40 MB hard disk space, depending on the operating system. The system also requires up to 700 MB of available hard drive space for each premastering directory the town plans to maintain.
- Memory – At least 512 MB of RAM.

For the ApplicationXtender Distribution Database Reintegration Workshtation

- Processor – Pentium 4 (A faster processor increases ApplicationXtender Distribution productivity)
- Available hard disk space – The ApplicationXtender Distribution Database Reintegration software requires about 25 MB hard disk space, depending on the operating system.
- Memory – At least 512 MB of RAM
- CD-ROM drive or drives or DiskXtender/MediaStor with a CD-ROM drive or jukebox – To reintegrate ApplicationXtender Distribution CD-ROMs and to provide access to ApplicationXtender Distribution CD-ROMs on the town's workstation or network, the town needs a CD-ROM drive or drives to read the ApplicationXtender Distribution CD-ROMs the town receives for the system. If the town chooses to store its copy of the ApplicationXtender Distribution CD-ROMs in DiskXtender, the town needs a CD-ROM drive attached to its DX MediaStor computer to read the ApplicationXtender Distribution CD-ROMs.

For the ApplicationXtender Media Viewer Client Workstation

- Processor – Pentium 4 (A faster processor increases ApplicationXtender Viewer productivity)
- Available hard disk space – ApplicationXtender Viewer software requires about 25 MB hard disk space, depending on the operating system.
- Memory – At least 512 MB of RAM for a retrieval workstation.
- CD-ROM drive with which to read ApplicationXtender Distribution Media – If the town is not using a reintegrated database, or if the town is using a reintegrated database on a standalone workstation, the town needs a CD-ROM drive to read the ApplicationXtender Distribution media you receive.

For the all other clients and admin.

- Processor – Pentium 4 (A faster processor increases ApplicationXtender Desktop productivity)
- Available hard disk space – Depending on the operating system and third-party components needed:
    - 12 MB (ApplicationXtender Admin)
    - 22 MB (ApplicationXtender Document Manager, including ApplicationXtender Data Source Selector)
    - 5300 KB (ApplicationXtender Import Archive and Migration wizards)
    - 5324 KB (ApplicationXtender AppGen)
    - 6108 KB (ApplicationXtender Image Capture)
    - ApplicationXtender Desktop also needs additional space on the drive to store temporary files during the installation process.

■ Memory – At least 512 MB of RAM (ApplicationXtender AppGen; ApplicationXtender Import Archive, and Migration wizards; ApplicationXtender Admin; scanning workstations; retrieval workstations)ddd

In summary, the software used for the town's ECMS is "Documentuam Application Extender", version 6.0. The current computer system being used is a Dell Opti-flex 755 Duo CPU 3ghz. The operating system is "Windows XP". The scanner is a Cannon DR5010C multi-page scanner that can scan up to 11"x17" pages. Printer is a HP Laserjet M2727 as well as a HP Designjet T1120PS color wide format printer and a KIP 3100 wide format scanner/printer.

Section 11: Updating the System

In an effort to ensure the authenticity of the electronic records contained in the town's ECMS, to ensure those records in the system are maintained for the legal retention period and to ensure the records are easily accessible, the town has purchased, from the vendor, the annual maintenance agreement for the software used to create and manage the electronic records in the system.

The vendor notifies the town of the availability of new releases of software. Generally a new version is released annually. The new release will include new features, as well as new listings of third-party product compatibility, including but not limited to operating systems and hardware.

The new features may at times also include modification of previous version features such as operating systems that no longer are supported under the new release. At that time, it will be the town's responsibility to upgrade its environment to meet the needs of the new release, as specified. The vendor will provide reasonable assistance to help the town install new releases. This work will also need to be coordinated with the town's IT personnel.

Section 12: Violations of the Standard Operating Policies

For information about the town's policy regarding violations of the policies and procedures described in this manual, staff should consult the Town of Batavia, Town Employee Handbook, Section 305, "Corrective Action and Discipline".

Section 13: Appendices

Appendix #1

The Town of Batavia ECMS Records Reference Policies

These policies have been established in an effort to offer guidance to staff providing access to electronic records on the town's ECMS and to ensure effortless and consistent public access to the electronic records contained in the town's ECMS.

1. Regarding the submission of a Freedom of Information Law Request (FOIL) – Individuals may submit a FOIL request for electronic records in the ECMS ether in writing or e-mail sent to the town clerk and records management officer who is also the records access officer for the town. .
2. Regarding public access – Individuals interested in obtaining access to the ECMS must complete a request form, which is appended to this manual. The public access terminal will be available Monday through Friday in the Batavia Town Hall Conference Room from 8:30 AM to 4:30 PM.
3. Regarding the use of outside media to obtain copies of electronic records on the ECMS – No outside media (zip drives, CDs, DVDs, etc.) will be allowed for use in a town computer. If the requestor would like the information to be provided on external media, the media must be purchased from the Town. CD-Rs and DVDs will be available for purchase.
4. The cost per page up to an 11"x17" document will be 25 cents per page. The cost for copies of larger documents will be calculated based on the actual cost to produce

those copies. There will be no charge for copies of electronic records provided by e-mail.

5. If a requested electronic record requires additional programming to retrieve the requested record(s), any charges for the additional programming to retrieve the requested records will be based on section 87(1)(c) of the 2008 amendments to the FOIL Law.
6. The cost for a CD-R, DVD, jump drive or other storage media to hold the requested electronic records from the ECMS will based on the most reasonable current cost for that media.

Appendix #2

Additional Information about New York's FOIL Law -

Under FOIL, the request for a record must reasonably describe the record and the town may require the request in writing [do you want to do that?].

Within five business days of receipt of a written request, the town must make the record available deny access to the record, in writing, with an explanation or acknowledge receipt of the request while noting the approximate date it will be granted or denied.

Denial of access to the record must be in writing and must state the statutory reason for denial and advise on the right to appeal the request.

It should be noted that records that are not disclosable under FOIL can be subject to a subpoena or a legal action of discovery.

Recently, there have been some amendments to the FOIL law which directly affect the electronic records placed on the town's ECMS.

The 2006 amendment to the FOIL law allowed for a requestor to ask for records by e-mail. In addition, this amendment indicated that if the town can scan the records and doing so will not involve any effort additional to another method of response, the town must do so. Further, as a result of this amendment, the law now indicates that if a court finds the town did not have reasonable cause to deny access, it can hold the town responsible for court costs and attorney fees.

The 2008 amendment to the law clarified issues that govern access to electronic records. Among those issues, the most significant ones are: (a) electronic records cannot be created in a way that impairs public access (access including both public inspection and copying) and (b) electronic records should be designed to allow the segregation and retrieval of information (to provide maximum public access). The second change reinforces the importance of having a good filing plan for the town's electronic records placed in the ECMS.

Other features associated with the 2008 amendment include: (a) the town cannot deny a request on the basis that the request is voluminous or burdensome, (b) the town can charge for access up to the hourly salary of the employee of the lowest rank who is able to retrieve the records and (c) additional programming necessary to retrieve an electronic record shall not be deemed the preparation or creation of a new record (which would be an exemption under FOIL).

Despite the formality of the FOIL law as stated above, as a part of the regular business of the town, it may be decided to handle some FOIL requests informally. In keeping with this thought, it should be noted that, generally speaking, all the town's records are considered open to the public unless someone or some organization can get hurt as a result of releasing records.

If the requested electronic records are not instantly available, or if the town needs time to thoroughly examine, or locate records then, the town will treat the *request as a FOIL request and deal with the request according to the FOIL law, providing the appropriate acknowledgement of the request.*

Appendix #3

The New York State Archives Imaging Production Guidelines

IMAGING PRODUCTION GUIDELINES

SCOPE: These guidelines list the minimum standards for producing and inspecting digital images of records. The term “large-scale architectural, engineering, and topographical drawings” refers to hard-copy documents in excess of 11" X 14" in size, consisting predominantly of lines, or to similarly formatted electronic equivalents. The term “office documents” refers to standard 8½ X 11", 8½ X 14", or similar sized paper documents consisting predominantly of textual data, or to similarly formatted electronic equivalents. The term “small-format pictorial documents” refers to documents of a size similar to office documents but which consist primarily of photographs, drawings, or other visual information. Where applicable, these guidelines follow national digital imaging standards and industry practices. All references to industry standards (ANSI, AIIM, etc.) are to the latest revision thereof.

IMAGE FORMAT: Requirements for image formats shall depend on the particular purpose of the image.

1.1 **Master Images:** Record copies of images shall meet these guidelines:

1.1.1 For black and white textual or line-art documents:

Format:	1-bit TIFF (latest version)
Tonal depth:	Bitonal
Compression:	Uncompressed
Spatial resolution:	At least 200 dpi (unenhanced true scan)

1.1.2 For black and white photographs or other pictorial documents:

Format:	8-bit TIFF (latest version)
Tonal depth:	Grayscale
Compression:	Uncompressed
Spatial resolution:	At least 200 dpi (unenhanced true scan)

1.1.3 For documents in which color is essential:

Format:	16-, 24-bit, or 36-bit TIFF (latest version)
Tonal depth:	Color
Compression:	Uncompressed
Spatial resolution:	At least 200 dpi (unenhanced true scan)

1.1.4 For backup images of the above, as applicable:

Format:	As applicable above
Tonal depth:	As applicable above

Compression:	Latest ITU standard compression preferred
Spatial resolution:	As applicable above

1.2 Access Images: User copies of images, if they must differ technically from the master copies, shall meet one of the following guidelines:

1.2.1 General Requirement (Alternative 1):

Format:	TIFF (latest version)
Tonal depth:	Bitonal, grayscale, or color as appropriate
Compression:	Allowed (latest ITU standard compression preferred)
Spatial resolution:	At least 200 dpi

1.2.2 General Requirement (Alternative 2):

Format:	JPEG (latest version)
Tonal depth:	Grayscale or color, as appropriate
Compression:	Allowed as needed, lossless compression for JPEG 2000 preferred
Spatial resolution:	At least 200 dpi

1.2.3 General Requirement (Alternative 3):

Format:	PDF/A with images using lossless compression preferred
Tonal depth:	Bitonal, grayscale, or color, as appropriate
Compression:	Allowed as needed
Spatial resolution:	At least 200 dpi

COMPRESSION: Maintain record copies uncompressed to ensure easy accessibility to the image over time. Compress access or use copies using non-proprietary, lossless compression algorithms. Document that lossless compression is being used. This will help ensure there is not a mixture of lossy and lossless images in the files.

SCALING: Scale access images so most documents fit within the typical computer screen or window for the given application. For instance, a particular application may require documents be scaled to half their size or less to comfortably fit a screen.

IMAGE HEADERS: Master images cannot have proprietary headers; including headers included in the PDF file formats, which make the images inaccessible except in particular software environments. Access images cannot have proprietary headers, except PDF headers where necessary.

IMAGE ORIENTATION: Upright (maintain portrait or landscape orientation as appropriate).

STORAGE MEDIA: Regardless of the media, master copies of images must be accessible for the records' entire retention period. The media shall depend on the purpose of the images stored.

6.1 Master or Backup Images: Store these images on computer tape, CD-Rs, DVD-Rs, or other digital storage formats, as appropriate.

6.1.1 The manufacture date of removable storage media shall be less than a year before first use.

6.1.2 Removable storage media shall have a pre-write shelf life of at least five years and a minimum post-write life of twenty years, based on accelerated aging test results that report on specific disc areas, such as those found in ANSI IT 9.21 CD-ROM.

6.1.3 Computer tape is strongly preferred when using digital images as the storage format for permanent records.

6.1.4 Discs used as storage media must comply with the applicable ISO standards, which specify how this type of media disc must store information and which allow the interchange of discs within different systems, such as ISO/IEC 13490-1:1995 ("Information technology—Volume and file structure of read-only and write-once compact disk media for information interchange") and ISO/IEC 20563:2001 ("Information technology—80 mm and 120 mm DVD-recordable disk").

6.1.5 The media should be examined at least twice a year to see if there is any degradation.

6.2 Access Images: Store these images on magnetic non-removable equipment (server), CD-Rs, DVD-Rs, or other digital storage formats, as appropriate. CD-RWs or DVD-RWs are not suitable.

MULTIPLE-PAGE IDENTIFICATION: All images in a single document shall be accessible and presentable in their original order and be clearly associated with each other as parts of a single document.

VENDOR QUALITY CONTROL AFTER SCANNING:

8.1 Inspection of the images by the vendor for quality shall verify the following:

a. Correct image filename (unique identifier)
b. Correct file format for each image type (master and access)
c. Image scanned at appropriate unenhanced dpi for each image type

d. Image oriented properly, whether landscape or portrait
e. Image is correct size (in pixels along both dimensions)
f. Image is not skewed
g. Image is not rotated or flipped
h. Image is neither too light nor too dark
i. Appropriate contrast within the image
j. No distortion of the image (this includes cropping)
k. No extraneous materials (fingers, fasteners, etc.) obscure the image
l. No noise or other problems in image file
m. Appropriate indexing terms associated with the scanned image
n. Ensure that the monitor where images are viewed is calibrated and is under controlled viewing conditions
o. Vendor must indicate what image viewer it used to view and evaluate the images
p. DPI must be verified by an independent program

8.2 Correction of unacceptable images shall consist of the following:

a. Correcting image filename
b. Deskewing, rotating, or flipping the image to correct its orientation
c. Adjusting brightness, contrast, or tone through rescanning
d. Rescanning, followed by a re-inspection of the new image
e. Updating index database to correct errors

8.3 Unacceptable modifications to the images include the following:

a. Sharpening the image
b. Retouching or despeckling
c. Dithering or quantization
d. Removing information from the images
e. Adding information to the images

RESOLUTION: Image sharpness shall be equivalent to the dots per inch (dpi) required for the original image type as explained above. Use commercially produced resolution targets, such as those outlined in ANSI/AIIM TR38-1996, “Identification of Test Images for Document Imaging Applications,” and following techniques in ANSI/AIIM MS44-1988 (“Recommended Practice for Quality Control of Image Scanners”) to verify scanner performance. Provide evidence of adherence to these standards at the close of the project.

DOCUMENTATION TO SCAN WITH THE RECORDS: Scan the following documentation with the records, ensuring that this documentation is clearly associated with this specific set of records:

a. State Archives Records Inventory Data Worksheet
b. File Information Form
c. Organization name and address

d. Contractor's name and address, and dates of scanning

e. Resolution Target that complies with ANSI/AIIM TR38-1996 ("Identification of Test Images for Document Imaging Applications") or other industry-standard resolution target

f. Indices, finding aids, and other metadata associated with the documents, if supplied by the customer (which differs from the index database for the images)

g. Annotations or "sticky notes" should be separate from the image and not burned onto the image file itself

RETRIEVAL AIDS: Indexing shall comply with specific requirements of the customer, but shall at the minimum include the following:

11.1. **Unique Identifier for Images:** Each image shall have a unique identifier, preferably sequential, which can be numeric, alphanumeric, or alphabetic as required by the customer. Each filename shall be unique across all separate external media, not merely within a single disc or tape. If required, file the documents in appropriate electronic folders.

11.2. **Indexing Data Fields:** The index of images shall consist of a limited number of field names to ensure adequate access to the records. Whenever possible, the field data shall consist of objective indexing terms (such as personal names, file numbers, social security numbers, etc.) rather than subjective data (such as subject terms).

11.3. **Optical or Intelligent Character Recognition:** If required, the vendor shall conduct optical or intelligent character recognition (OCR or ICR) to convert digital images into electronic text. The vendor shall certify the conversion to be at least 99.9% accurate as measured by character count, and the converted text shall be associated with the respective digital image or document. This percentage is equivalent to 10-20 errors per page on a standard 2000 character page when character and formatting is taken into account.

11.4. **Indexing Database:** The indexing database (including, if applicable, OCR text) shall store the required index data in ASCII or Unicode, and each record within the database shall be associated with the respective digital image or document.

11.5. **Index Accuracy:** The vendor shall verify the index via dual data entry, data entry operator verification immediately subsequent to data entry, or other means as appropriate, to ensure accuracy.

PACKAGING: Optical media (CD-Rs, DVD-Rs, etc.), if used, shall be in unbroken jewel cases and shall rest on the inner spindle without pressure that could produce damage during removal or re-emplacement. Tapes and other media, if used, shall be in individual containers of the appropriate size for the particular media. The customer may accept or require alternate packaging as suitable. The vendor shall deliver separated sets of master and duplicate copies of media to the customer in boxes, with the media fitting firmly but not tightly.

PACKAGE MARKING: At a minimum, the following data should be machine printed on label on each jewel case or other storage container of both the originals and the backups:

Organization Name
Records Series Title and Date
Range of Records (if appropriate)
Package or Media Number

QUALITY OF WORK: Scanning shall capture each digital image of a document page so that every line and character on the document appears and is legible in the image. Removable media shall be free of scratches, cracks, finger marks, warping or any other defect that might adversely affect quality or usability.

CONTRACTOR INSPECTION: The vendor shall inspect each individual image, disc, tape, or other storage medium for compliance with the requirements herein, including resolution, image quality, accuracy of the index, and general workmanship. The vendor shall include an inspection report or certification covering each disc, tape, or other storage medium included in each shipment.

CUSTOMER QUALITY CONTROL: The customer shall have the right, after inspection, to reject any images determined not to meet the requirements of these guidelines. In such cases, the contractor must rescan at its expense.

REJECTION OF BACKUP MEDIA: When the customer or its inspection agent (if applicable) rejects an entire disc, tape, or other storage medium, the customer or vendor may deface the rejects by cracking, punching, or shredding. The customer may retain rejected media at its discretion.

VENDOR FACILITY INSPECTION: The customer reserves the right to inspect and approve the vendor’s work site before and at any time during the performance of a contract to ensure the vendor’s production and quality control capabilities. An inspection of the vendor’s facilities is always recommended.

FILE INTEGRITY: Unless otherwise specified elsewhere in the contract, the vendor shall maintain the original documents in their existing file order before, during, and after scanning. The vendor shall return file material to the original storage containers in the same order that existed before scanning, except that the vendor shall maintain any corrections to file order made during the preparation for scanning. The vendor shall not restore any fasteners (staples, clips, tape, etc.) removed during document preparation.

Appendix #4

Resolution Adopting the ECMS Standard Operating Procedures

Appendix #5

Resolution Appointing the Town of Batavia Records Access Officer

Resolution No. 99 dated June 16, 2010 amending resolution 1 of 2010; GENERAL ORGANIZATIONAL RESOLUTION, resolved to amend resolution number 1 of 2010 by adding the following:

OFFICE/DESIGNATION	APPOINTEE
RMO/RAO………………………………………	Teresa M. Morasco

Offered by: Councilman Gerace
Second by: Councilman Deputy Supervisor
Ayes: Gerace, Lang, Underhill, Michalak, Post
APPROVED by unanimous vote (5-0)