NUMBER

85

Developing a Policy for Managing Email

By
Ann Marie Przybyla

2010

New York State Archives

The University of the State of New York
The State Education Department
New York State Archives
Government Records Services
Albany, New York 12230
www.archives.nysed.gov

THE UNIVERSITY OF THE STATE OF NEW YORK

Regents of The University

MERRYL H. TISCH, *Chancellor,* B.A., M.A., Ed.D.	New York
MILTON L. COFIELD, *Vice Chancellor,* B.S., M.B.A., Ph.D.	Rochester
ROBERT M. BENNETT, *Chancellor Emeritus*, B.A., M.S.	Tonawanda
SAUL B. COHEN, B.A., M.A., Ph.D.	Larchmont
JAMES C. DAWSON, A.A., B.A., M.S., Ph.D.	Plattsburgh
ANTHONY S. BOTTAR, B.A., J.D.	Syracuse
GERALDINE D. CHAPEY, B.A., M.A., Ed.D.	Belle Harbor
HARRY PHILLIPS, 3rd, B.A., M.S.F.S.	Hartsdale
JAMES R. TALLON, JR., B.A., M.A.	Binghamton
ROGER TILLES, B.A., J.D.	Great Neck
KAREN BROOKS HOPKINS, B.A., M.F.A.	Brooklyn
CHARLES R. BENDIT, B.A.	Manhattan
BETTY A. ROSA, B.A., M.S. in Ed., M.S. in Ed., M.Ed., Ed.D.	Bronx
LESTER W. YOUNG, JR., B.S., M.S., Ed.D.	Oakland Gardens
CHRISTINE D. CEA, B.A., M.A., Ph.D.	Staten Island
WADE S. NORWOOD, B.A.	Rochester

Commissioner of Education
President of The University of the State of New York
DAVID M. STEINER

Deputy Commissioner for Cultural Education
JEFFREY W. CANNELL

Assistant Commissioner for New York State Archives
CHRISTINE WARD

Director of Operations
KATHLEEN D. ROE

Director, Government Records Services
GEOFFREY A. HUTH

This publication is distributed by the New York State Archives. If you have any questions concerning its contents, please call (518) 474-6926, or send an email to the State Archives at archpubs@mail.nysed.gov

Table of Contents

Executive Summary

Until now, most organizations have failed to include email in a formal management policy or program. This omission is no longer acceptable, because email can be a record and an information asset, email can be used as evidence in a court of law, and failure to control email can be very costly.

These guidelines are intended as a starting point for state agencies and local governments to use for writing policies and procedures that will guide a program for managing email. Agencies and governments should adapt the guidelines to meet their own needs and capabilities, and continue to update their policies on an as-needed basis.

Principles and Best Practices

Some general principles and best practices for managing email are listed below and are discussed more fully in Section 2 of these guidelines.

1. **Understand email use,** develop strategies that are selective, and focus resources where they are most needed.
2. **Manage centrally,** reducing reliance on the end user.
3. **Manage electronically** as much as possible, reducing reliance on users and manual management strategies.
4. **Ensure cooperation,** coordination, and support; that is, ensure the cooperation of all users of the email system, the coordination of several key individuals throughout the organization, and management support.
5. **Address any backlog** by developing a strategy that is based on solid reasoning and a rational disposition strategy and that is documented in an email management policy.

Components of a Policy

Any policy that governs an email management program must address—but not necessarily be limited to—the following points (see Section 3 for more detail):

1. **Essential elements** of the email management system: What are the system capabilities and functions? What information and records are in the system?
2. **Classifying email:** Which emails are records? Which emails are not records for legal purposes? What are the required security levels, filing rules, and indexing fields?
3. **Access and retrieval:** How do users find emails? How can users enhance access? To which emails do users have access? How will access be

provided to the public? Under what circumstances is access denied to the public?

4. **E-discovery:** What is the process of responding to impending litigation? Who initiates the response? How and when is the process initiated?
5. **Storage:** What is the range of storage options used? How long will emails remain on the server? When, if ever, are emails transferred to removable storage media?
6. **Retention and disposition:** What are the retention periods for different types of emails in the government or agency? How is retention managed? When and how are obsolete emails destroyed?
7. **Preservation:** How are long-term and permanent emails preserved? What formats and media are used? How does the government or agency track and manage migration? How does it ensure media integrity? How and when does a state agency transfer archival emails to the State Archives?
8. **Information security:** What technical and procedural measures are in place to ensure information security?
9. **Appropriate use:** How does the government or agency define the appropriate use of email? How are these principles disseminated? How is appropriate use monitored? What are the measures for addressing misuse?
10. **Staff training:** How is staff trained on the email management policy? What subject areas are addressed?
11. **Roles and responsibilities** must be clearly assigned and defined for each of the above components.

Included in Section 4 of the guidelines are three sample policies that reflect the needs and capabilities of three sizes of government or agency. The sample policies illustrate how to use current best practices (Section 2) to integrate and address the above components (Section 3) in a policies and procedures document.

1. Introduction

1.1 Purpose and Intent

Few governments or agencies have focused on email when it comes to policy and program development. Email systems have been implemented at all levels of government throughout New York State to meet immediate business needs, but the smooth operation of these systems has been viewed as a function of information technology (IT) rather than of records management, administration, legal compliance, or internal control. Email is generated by and maintained in a software environment that is not intended for long-term storage. Many users have equated email with a telephone call: ephemeral, private, and exempt from oversight. The truth about email is much different.

Legislative changes and high-profile court cases of the past decade have firmly established that email can be an official record, email can be used as evidence in a court of law, and failure to control email can be very costly. In New York State and elsewhere, state agencies, professional organizations, vendors, and public and private partnerships offer educational programs about how to manage electronic records and email. Organizations have access to a growing range of technological solutions for managing email, as software developers and vendors have increased their efforts to meet a critical business need. Claiming ignorance as an excuse for not implementing an email management program is no longer an option (and legally never was).

This set of guidelines is not an overarching New York State policy on managing email. Rather, these guidelines reflect current principles and best practices for managing email, and are intended as a common starting point for state agencies and local governments to use for formulating their own internal policies on email management. Agencies and governments should adapt the guidelines to meet their own unique needs and capabilities.

Issues regarding email will continue to change, undoubtedly becoming even more complex as our reliance on mobile technologies continues to grow and we stand even more firmly in the electronic world. For these reasons, the State Archives will review these guidelines periodically and update them to ensure they reflect current laws, practice, wisdom, and capabilities. Similarly, all local governments and state agencies must periodically review and update as needed their own email policies and procedures, regarding them as living documents, as dynamic and prone to change as technology itself.

1.2 Structure and Contents

As a product of the State Archives, these guidelines as a whole address how records management laws and principles apply to email. The guidelines also highlight email best practices that have recently emerged, many spurred on by legal changes and made possible by advances in technology.

These guidelines are divided into the following sections:

Executive Summary: States the central principles that should guide policy development for managing email.

1. **Introduction:** Provides the intent of these guidelines, a brief outline of how the guidelines are organized, and definitions that are essential for examining the challenges of and strategies for managing email.
2. **Principles and Best Practices:** Discusses best practices that are emerging after a decade or more of email use in the workplace.
3. **Policy Components:** Describes the basic elements to include in any policy for managing email.
4. **Sample Policies:** Provides three samples that illustrate the management strategies, needs, and capabilities of governments and agencies, from the smallest local government to a large state agency.

Appendix: Provides a short discussion of state and federal laws and regulations relating to records management, especially the management of electronic records (including email).

Sections 1 through 3 and the appendix are intended to give context and meaning to the three sample policies, while the three sample policies in Section 4 demonstrate the range of strategies available for managing email. The samples are not meant to suggest, however, that only three strategies are possible. Future revisions of these guidelines may expand to include actual policies and procedures from sample email management programs in New York State.

1.3 Terms and Concepts

Managing email over the long term is challenging because of email's essential characteristics. An email originates in an *electronic format*, but it can also exist in a specific type of computer file or *file format*. Email tends to reside in a *proprietary* file format in an email system; although there is interoperability between email software systems, email exists as a file format that is owned and controlled by a single software company and is not necessarily (or easily) exportable to another environment. For these reasons, long-term or permanent emails must be created in or converted to non-proprietary formats for preservation (for example, Extensible Markup Language, or XML, which is explained in Section 3.7, "Preservation").

Most emails conform to an international *style format* known as RFC 2822, which defines an email as consisting of a *header* (routing information) and a *body* (the message), which are separated by a blank line. The body of the message can conclude with a signature block. Saving emails as plain text (ASCII, Unicode) does not necessarily preserve the style format and general appearance of email; additional measures may be needed to display an email as it was originally created.

Metadata refers to any information describing a set of data. Metadata can be viewed in the header of a single email, but for every email there is also a more detailed *file profile*, also known as a *document profile*, which is a hidden, associated page of information about that email (see, for example, the "Properties" tab in a GroupWise email). Metadata provides the context for an email (sender; recipients; dates transmitted, opened, deleted), identifies the email's subject content and software environment, and indicates any modifications that were made after the initial transmission. For these reasons, the continuing association of metadata with its email message is essential for ensuring the long-term accessibility and legal admissibility of a message.

An *attachment* is an electronic file that is associated, sent, and received along with an email message. Attachments may be text documents, graphics, spreadsheets, video and audio files, webpages, and compressed or encoded files. The number of possible file formats attached to an email is essentially as unlimited as the number of formats that currently exist. Again, for preservation, access, and legal purposes it is essential that the attachment continues to be associated and retrievable with the original email message, as well as with all metadata for the message and the attachment.

Discovery refers to the compulsory disclosure of documents that may be relevant to a legal inquiry. *E-discovery* involves records in electronic format, and emails are discoverable because they can be—and routinely are—the focus of an e-discovery action. The courts have increasingly emphasized the importance of having a records management program that is regulated by policy, and that policy must extend to managing email, for both electronic discovery and record admissibility purposes.

2. Principles and Best Practices

2.1 Understand Email Use

When trying to manage email, there is usually no easy solution. Managing email means developing strategies that are selective, focusing resources where they are critically needed and where they will have the greatest impact. Policy decisions on how to manage email must reflect how a government or agency uses email. For example, do users primarily use email to communicate short, transitory messages, with some isolated exceptions? Or does a government or agency, or an individual unit of that government or agency, rely on an email system to send, receive, and store records relating to one or more core functions? The extent to which an email system is used for transmitting and receiving records, the distribution of records across a government or agency, and the value and retention requirements of those records must guide policy and the management strategy.

2.2 Manage Centrally

Email policies of the past decade have tended to make individual users responsible for managing their own emails. Recent litigation and studies have highlighted the shortcomings of this approach in guaranteeing organization-wide compliance with records and other requirements. In large organizations especially, email is managed inconsistently if left to end users, because individuals exercise various levels of discipline and use their email accounts differently.

Central control is necessary to eliminate unnecessary duplicates, identify and link threads in an extended email exchange, provide access to more than one user, and guarantee legal compliance. These guidelines tend to emphasize (and encourage) strategies that allow some degree of centralized control, at least for emails that are permanent, vital, or vulnerable to e-discovery. Email management may be centralized agency-wide, government-wide, or by individual program units.

Options for managing email centrally include

- managing via a Local Area Network (LAN), or a shared directory. A LAN, or shared directory, is an imperfect tool for managing emails centrally, because it ultimately relies on each user of an email system to move individual emails manually out of a mailbox and into a shared electronic file system.
- email archiving software, which captures and preserves email traffic flowing into and out of the email server and stores it at a central location. Email archiving provides "single-instance storage," meaning that only one copy

of an email or attachment is stored in the archive but is associated with senders and receivers, thereby reducing the volume of email on the online email server and making search and retrieval more efficient. Email archiving does not, however, integrate email with other electronic records (word-processed files, databases, webpages); emails exist and are managed as a stand-alone body of information.

- Electronic Document Management System/Enterprise Content Management (EDMS/ECM), which is a central repository for all electronic records. Depending on the product, an EDMS/ECM can have a sophisticated array of management functions, and can even manage retention and disposition through a records management application (RMA). Email management exists as a separate, add-on module of an EDMS/ECM.

2.3 Manage Electronically

Another management strategy has been to rely on the "low-tech" method of printing out important emails to integrate them into a paper recordkeeping system. Printing emails is still a viable option for a small organization with limited technology support and finances, provided that individuals across the organization consistently apply records retention requirements to the printed emails, capture all essential metadata, and file the emails with their respective attachments. Such controls are difficult, if not impossible, to enforce in large organizations where email traffic and volume is increasing exponentially.

Governments and agencies are more likely to ensure compliance with policy by retaining their email electronically and managing their email records with a growing arsenal of electronic tools (although it may still prove necessary to print emails occasionally, to integrate a few emails into an existing paper file).

2.4 Ensure Cooperation, Coordination, and Support

Most local governments and state agencies are required by law to appoint a records management officer (RMO), who is responsible for coordinating and overseeing a comprehensive records management program. It can be difficult to coordinate and gain support for managing a resource that affects everyone, especially in an environment with a mixture of full- and part-time officials and employees, interns, volunteers, and contractual personnel working at various locations. Because of the impact and costs of not managing email, however, RMOs and others in governments and agencies must develop strategies and mechanisms for building cooperation.

The management of electronic records and email can enhance the relevance and visibility of a cooperative body that already exists in a local government or state agency, or it can be a compelling reason for initiating a cooperative body that includes everyone with an interest in and knowledge about

records. Possible responsibilities of such a board or committee could be to

- ensure communication between program areas that are directly concerned with electronic records (especially records management and information technology)
- advise on the desired capabilities of a software solution to manage email and other electronic records
- review requests for proposals (RFPs) and responses to the RFPs for email management solutions
- coordinate an appropriate response to a legal action or other inquiry (FOIL, audit)
- identify sources of grant funding, and identify and prioritize projects for grant applications
- identify and coordinate training opportunities
- periodically review policies and procedures for managing electronic records
- advise on appropriate responses (including disciplinary measures) when policies and procedures aren't followed

An RMO in a local government can form, refocus, or re-energize a records advisory board to advise on electronic records issues, or form a technology committee to focus on the unique needs of electronic records. An RMO in a state agency can form or give a new role to a committee that consists of liaisons from across the agency who are directly involved with managing records in their respective program areas and with coordinating those functions with the RMO. The records manager, records access officer, information technology director, information security officer, and legal counsel should be involved in any such committee, working with the support of and input from management.

2.5 Address Any Backlog

Many local governments and state agencies are dealing with a backlog of unmanaged emails stored either on servers or on various storage media offline. Whether or not to manage emails retroactively depends on the level of risk involved in not managing them. If the risk level is high, analysis of a sample of tapes or other storage media involved might suggest an appropriate course of action. Methods of analysis may include

- downloading backups or copies of email into an existing management system
- working with a data recovery vendor to restore tapes or other media one by one
- surveying past email users to determine what is likely to be on the media

The goal is to identify, as much as possible, the latest retention period of records on the storage media and to destroy the media when that retention period has passed. Base all strategies on solid reasoning, and document those strategies in an email management policy.

2.6 Work with Service Providers

A variety of services are available to governments and agencies that either don't have or can't afford to divert their limited resources towards managing email entirely on their own. These services include

1. Commercial Internet Service Providers (ISPs), who provide email services as a component of Internet services (such as Verizon, Time Warner)
2. Widely used commercial stand-alone email systems (such as AOL)
3. Free email services (such as Gmail, Hotmail, Yahoo)
4. Email services offered by local governments or state agencies (BOCES for constituent school districts, counties for municipalities, Office for Technology for state agencies and others)

It is important to define in policy the range of email services received from an outside service provider. Whenever possible, arrange for services that extend beyond connectivity to include essential management functions. In addition, be aware of potential problems involving the use of the first three options listed above, such as limitations on attachment file size and mailbox capacity and the difficulty of importing files from the host system. A signed contract or service agreement with the outside provider should reflect the system's capability to address existing policies and procedures.

Managing email consistently and comprehensively can be problematic when individual users in the same government have accounts with several different services or service providers. One solution is to download all government email records to a central server, where email records can be stored in-house and managed electronically through the use of specialized software. The alternative is to work with the email service provider to utilize "software as a service" possibilities to ensure that all aspects of email, including retention and disposition, are managed appropriately while not making further demands on an in-house technology infrastructure.

3. Policy Components

3.1 Essential Elements of the Email Management System

An email policy documents the email management system at a particular point in time. The system contains certain types of information that may or may not be records, as defined by law, so the policy must describe how the system is used and the information and records it contains. This will determine the way the system works.

3.2 Classifying Email

An email must be managed according to how it is defined in terms of the information it contains. To meet basic records management requirements, emails must be evaluated at three levels.

- *Is an email message a record?* An email is a record if it is created or received as part of a business transaction of a government or agency. Email messages that are records include policies and directives; correspondence or memoranda related to official business; work schedules and assignments; agendas and minutes of meetings; documents that initiate, authorize, or complete a business transaction; and final reports or recommendations. Emails that are not records include general listserv messages, spam, broadcast messages received by staff, and personal messages.
- *If an email is a record, to which records series does it belong?* Local governments should consult an appropriate State Archives' records schedule to answer this question. State agencies can consult the state general records schedule or an agency-specific records schedule to determine the records series.
- *What is the retention period for that records series?* The answer to this question dictates the basic records management requirements (for example, the access, storage, and preservation needs) of that email.

Options for classifying emails include

- manually: relying entirely on an individual user's knowledge of work processes
- semi-automated: using software that prompts users with a checkbox to classify emails before closing or saving
- fully automated: using software that reads, categorizes, and files email, based on business rules that reflect how an organization uses email

Each of the above strategies will have varying degrees of compliance and accuracy and differing implementation costs, depending on the controls in place to support the classification system and the size, cultural environment, and technical capabilities of an organization.

3.3 Access and Retrieval

Enhancing access and retrieval

Filing has typically been viewed as a way to enhance access, and file folders traditionally are arranged by work function, subject, or date, or a combination of these intended to aid retrieval. However, in an electronic environment, a search engine can reduce or eliminate the need for a filing structure to find records (although electronic filing systems can still be useful for other reasons, such as managing retention, as discussed below).

To make searching more efficient, individual users must always assign a subject line to outgoing emails, and can even assign one or two index terms (a case number, for example) to the subject line or metadata of each email record they send and to the metadata of each email record they receive. This requires a controlled vocabulary, naming conventions, training for individual users, and discipline. It may be possible to adopt this as a strategy only to manage important or vital email records or those records that may be relevant to legal proceedings.

Restricting access

Conversely, there should be mechanisms in place to restrict access to certain emails or even parts of emails. Access to emails relating to law enforcement investigations, court actions, and personnel and health matters may be restricted, sometimes by law, to a few designated individuals in a government or agency. If emails are routed to a central filing system, it's important to implement system security measures that restrict access to certain directories, file folders, and individual files by job function or title. Email users should have read-only access to stored emails to ensure the legal admissibility and integrity of the records.

Because of the nature of email conversations, a single email can begin with one subject and end with another, and one part of an email may be restricted while another part is not. Governments and agencies should therefore be prepared to produce redacted versions of emails, to provide access to the unrestricted information in an email (in response to a FOIL request, for example). No matter what kind of method of redaction is used, it must be subject to a verification and quality control process, to ensure that the redacted text is truly irretrievable by unauthorized users.

3.4 E-discovery

A government or agency may decide to develop a separate, highly detailed set of e-discovery policies and procedures because of the complex legal issues involved in an e-discovery action. This is important, since the failure to respond appropriately can result in legal sanctions, loss of reputation, and other significant costs.

An e-discovery policy must stipulate that if someone in a government or agency knows of an impending legal action, that individual must notify legal counsel immediately. Because records are increasingly electronic, legal counsel must, in turn, contact the records management officer and the lead information technology professional (either a consultant on retainer, program area director, or chief information officer) for two reasons: to understand the information technology environment, and to know the content and format of potentially relevant electronic records.

The more information available to legal counsel beforehand, the better. Ideally, legal counsel should know, or have the resources available to discern quickly, how an agency or government uses email and the types of records likely to reside in the email system.

3.5 Retention and Disposition

Simplifying retention

Purging all emails after a defined time period is not an acceptable retention and disposition strategy. Each email record belongs to a records series that is included (or needs to be included) in an official retention schedule. In today's business environment, it is highly unlikely, if not impossible, that a government or agency would transmit only emails that are non-records or that have a retention period of "0 after no longer needed."

It is possible, however, to simplify retention and manage emails as groups of messages belonging to a cluster of records series with similar retention periods. First, the RMO and other government officials must know the retention requirements of emails transmitted within their government or agency. State agencies must determine whether emails are part of records series that have been or need to be scheduled. Retention strategies can then be applied selectively, according to the retention periods of emails transmitted and received by individual users, program units, or a combination of these.

Some email management strategies include

- identifying those units that transact business almost entirely by email (for example, a contracting unit that collects responses to RFPs strictly via email), and then focusing an automated solution on those units and their records

- focusing on the emails of individuals in upper levels of management or occupied with certain job functions (legal, health, human resources, construction, land use), on the assumption that their records are long-term
- identifying and removing permanent emails from individual accounts and managing them separately, while retaining non-permanent emails for the longest retention period short of permanent. For example, local governments can assess whether their emails are equivalent to correspondence. If so, they may apply the three retention periods for correspondence in the local government schedules (permanent, six years, 0 after no longer needed), separating out the permanent emails and destroying the non-permanent emails after six years. If local governments adopt this strategy, they may still need to identify a small number of emails that do not qualify as correspondence and save those emails for the full length of their respective retention periods.

Backups

It is important to follow a State Archives' retention schedule (either the general schedule for state agencies or a relevant local government records schedule) for email system backups. These can be subject to e-discovery, even if the original emails have been destroyed and especially if the court deems the originals were destroyed inappropriately. Conversely, the destruction of backups assumes that original emails were managed appropriately and destroyed according to State Archives retention schedules.

Attachments

An email may have a different retention period than its attachment. If an email is used essentially as a cover letter with a minimal retention period, the email and its metadata are still important for documenting that something was sent and received, which may prove relevant to legal and other inquiries. For this reason, as well as for the sake of simplicity, retain the email and the attachment for the longer of their two retention periods.

Copy control

Controlling copies is a retention issue, because retention requirements vary according to whether or not a record is the official copy. The concept of "official copy" is problematic when dealing with email because of the volume of emails, the difficulty of controlling all copies, and the occasional need to prove an email was received as well as sent. As with other retention issues, it's best to simplify copy control as much as possible.

The recipient's copy of an email received from someone outside of the government or agency is usually the official copy of the government or agency that receives it. The official copy of an email sent internally, however, may be the sender's or recipient's copy, may be both the sender's and recipient's copy, or may depend on whether or not the email is part of a larger series of records. In instances where several individuals participate in

an extended email conversation, the record copy would be the concluding message that includes all of the related threads of the email exchange, but it may be impossible to ensure that the whole, all-important thread is saved intact. Governments and agencies may therefore decide to save all copies of emails relating to certain critical issues or received by individuals who are likely to be involved in those critical issues. Again, this will involve analyzing and devising a strategy based on email use and the function of a program unit or department.

3.6 Storage

While the cost of electronic storage is steadily declining, the use of electronic technologies and the sheer volume of emails are increasing. In a small organization where email is used strictly for communication, managing storage may involve no more than deleting emails from the email server after the appropriate retention period for each specific message has passed. In more complex situations, however, emails may pass from active space on an email server to central storage, then to long-term storage, and eventually to external storage media. An email policy must document how the local government or state agency utilizes storage, to ensure that upgrades and migration address all long-term emails, regardless of where they reside.

3.7 Preservation

New York State law and regulations require that governments and agencies ensure that records are accessible for the full duration of their retention periods. For electronic records, including email, preservation of even short-term records can be problematic because of the pace of technological obsolescence and media degradation. Preservation strategies for email include

- using standard file formats to save messages, attachments, and the links between messages and attachments. Extensible Markup Language (XML) is quickly becoming the standard for managing long-term email and its associated metadata and attachments. XML is an open format and markup language that was developed to store and transport data between operating systems. XML uses tags to indicate the structure of data in an email, but it requires another software program to process the XML tags and display the data as an email message with an attachment.
- adopting open-source products and formats as much as possible to facilitate migration or conversion to a new email system
- assessing the need to migrate emails to a new system, and migrating minimally to balance concerns for data loss, costs, and long-term preservation. The more messages requiring conversion, the higher the costs. It's best to migrate a minimal volume of emails, which is possible only by applying effective, appropriate retention practices and destroying obsolete emails.

3.8 Information Security

The security of an email system is a shared responsibility. Information technology personnel, either in-house or outsourced, are usually responsible for implementing technical security measures, including firewalls, spam filters, anti-virus software, levels of access to applications and files, and passwords. Technology is, in turn, supported by clearly stated security policies and procedures, an ongoing training program for all email users, and a system of audits and correction.

In addition, state agencies are required to have an information security officer (ISO), according to the *Cyber Security Policy* (P03-002) issued by the New York State Office of Cyber Security and Critical Infrastructure Coordination (CSCIC). The ISO is responsible for building an "information security infrastructure," that is, implementing and overseeing an agency security program that is guided by policy. The ISO also monitors compliance with the security policy and enforces corrective action.

The other tenets of CSCIC's policy on information security apply to all state entities and to information assets that are shared between state and local governments. The policy is, however, a sample that local governments can apply to their entire information technology environment. The security policy is available on CSCIC's website, and local governments and state agencies should contact CSCIC for specific questions concerning Internet and email security.

3.9 Appropriate Use

The appropriate or acceptable use of email is a security issue. Without a use policy, a government or agency can be held liable for damages if an individual on staff sends or receives inappropriate messages. At the very least, the inappropriate use of email internally can cause disagreements between staff and a decline in productivity, and if transmitted externally can be damaging to an agency's or government's reputation. Downloading or opening inappropriate files can cripple an entire electronic system. An appropriate use policy places the burden of responsibility on the individual user rather than on the agency or government.

The principles of appropriate use are as follows:

- Confine use of government-owned computers and accounts to government business.
- Respect others' privacy, gender, sexual orientation, race, creed, ethnic background, or other identifying characteristics.
- Protect data from unauthorized use or disclosure as required by state and federal laws and regulations.

- Respect the value and integrity of computing systems.
- Safeguard individual users' accounts and passwords.

Elements of an organization's email policy should be integrated into existing webmail and network access policies to strengthen and give visibility to the email policy. The appropriate use policy should describe the disciplinary measures that would result from inappropriate use of the email system.

3.10 Staff Training

Training is an essential element in proving the legal admissibility of email records. The courts have concluded repeatedly that a poorly implemented policy is worse than no policy at all, and that an aggressive, ongoing training program demonstrates an organization's commitment to its own email policy.

Training falls into two broad categories that are not mutually exclusive. To use email effectively, all users must undergo training on the technical capabilities of the email program and on their role in maintaining system security. Training should also address all of the records issues involved with managing email, especially the functions for which users have direct responsibility. In small organizations, the records management officer can provide or arrange for training.

In large governments and agencies, responsibility for training may be divided among several staff and program areas: IT staff provide technical training (capabilities of and how to use the system), the information security officer coordinates and provides training on system security (including use of passwords and appropriate use), and the records management officer addresses records management issues (especially records retention and disposition). All local governments and state agencies can draw on the services of the State Archives to assist with their educational efforts.

As a followup to training, there should be a system of monitoring use to ensure compliance with email management policy and procedures. Governments and agencies have the right to monitor use, access individual accounts, and take corrective action as needed.

3.11 Roles and Responsibilities

For an email policy to be effective, it must clearly assign responsibility for all of the above aspects of managing email. The key players in managing email in a local government and state agency include the RMO, records access officer, information technology professionals, legal counsel, managers, and the email users themselves. As noted, state entities are also required to have an information security officer (ISO) and chief information officer (CIO), who

are responsible for aspects of email management in addition to their other responsibilities.

As applicable, email policy may articulate the respective roles and responsibilities of other levels of government, businesses, consultants, and state agencies. For example, the email policy of a state agency may stipulate that the agency will transfer all archival email records to the State Archives for permanent preservation in accordance with approved records retention and disposition schedules.

In large governments and agencies, key individuals or program units may assume responsibility for developing separate policy statements that together form a comprehensive email policy for the government or agency. For example, the administrative unit may develop the section of the policy on acceptable use, the information security officer may address the policy on passwords and against sharing email accounts, legal counsel may write detailed policies and procedures for e-discovery, and the records manager may address recordkeeping requirements or integrate emails into an existing records management policy framework. It is ultimately the responsibility of management or the governing board to support and promulgate email policies and procedures throughout the organization.

For More Information and Assistance

The State Archives provides direct advice to state agencies and local governments on all aspects of managing email, including setting retention periods and developing management policies for email. The Archives has regional advisory officers and Albany-based staff who perform site visits, provide technical advice and assistance, and present workshops on a wide variety of records management issues. Local governments are eligible to apply for funding through the Local Government Records Management Improvement Fund (LGRMIF) to implement various records management projects, including projects to inventory and manage their email. For further information, contact your regional office or the following:

Government Records Services
New York State Archives
State Education Department
9A47 Cultural Education Center
Albany, New York 12230
(518) 474-6926

4. Sample Policies

4.1 About the Sample Policies

This section consists of three sample policies that represent the range of government entities in New York State and the differences that may exist between policies of different types and sizes of organizations. The sequence of the policies represents a progression, from a small organization to a large organization, from a mostly manual system to a system that is almost fully automated, and from a simple policy to a policy that is necessarily more complex.

Policy 1: Village of Hidden Valley

This sample policy is written for a small local government with limited technical capabilities and in-house information technology support. The village's email management system consists of an email server that interacts with a freestanding email archiving appliance. Village staff are responsible for identifying and moving all permanent email records from the email server to a shared file directory, where they are managed with other permanent electronic records. The archiving appliance stores all emails for six years. Several village officials use personal email accounts on their home computers for village-related activities, and the policy includes procedures that address emails on home computers. (The State Archives discourages the use of personal email accounts to conduct public business. In smaller governments, however, this situation may be necessary, especially if board members and other officials do not have an office in a government facility.)

Policy 2: Town of Big Thunder

This sample policy is written for a medium-sized town. It assumes that the town owns an email management system with fairly robust capabilities and has an in-house IT director. The system requires town email users to classify incoming and outgoing messages manually, but then the system files the emails according to how they were classified. The system performs some retention and disposition functions, but does not destroy email records once they have passed their retention periods. The IT director implements destruction outside of the system. In addition, a small number of town officials use email accounts on their home computers for town-related activities. In this case, to discourage the use of personal accounts, the town provides email accounts on the home computers of a small number of town officials.

Policy 3: State Office of Administrative Support and Analysis

This sample policy pertains to a state agency. This agency has an in-house information technology staff, many different program areas, and a large, geographically dispersed staff. The policy that governs the agency's email

management system is necessarily more complex than the policy for a small or medium organization, and responsibility for maintaining the system and implementing policy is divided among a larger number of staff. The agency has explicitly prohibited the use of non-agency email accounts and computers for transmitting or receiving work-related emails, although there are provisions, documented in policy, for accommodating staff who travel or telecommute.

4.2 How to Use the Sample Policies

Please note that there are no actual municipalities in New York State called Hidden Valley or Big Thunder, nor is there a State Office of Administrative Support and Analysis. The sample policies for these fictional entities are divided into sections that reflect various aspects of managing email (as outlined in Section 3 of these guidelines). Each section begins with a policy statement, which is then followed by a list of procedures required to carry out that policy.

The State Archives is not promoting or recommending any of the electronic management systems that are featured in the three sample policies. Our goal is to present situations that are realistic and, therefore, sample policies that are useful to our customers.

Do not feel compelled to adopt the policies and procedures for one of the scenarios described above. Instead, use the samples to guide your decisions about the kind of information that may be important for you to include in your own email policy. Governments and agencies should adopt a solution that has as its end result the effective management of all aspects of email (retention and disposition, in addition to access). Develop a policy and procedures manual that best suits your particular needs, either expanding, simplifying, or combining elements of the samples provided in this section. Finally, these samples are not intended to be mutually exclusive. In some cases, a small local government may have a sophisticated system and therefore need a more detailed policy similar to the third sample, or a state agency may choose to adopt simplified strategies outlined in the first two sample policies.

Sample Policy 1

Village of Hidden Valley: Email Policies and Procedures

Effective October 2008

1. General Policies

The village legally owns all emails that employees and officials create and receive when conducting village business, regardless of where employees and officials create and receive the emails. Employees and officials have no promise of personal privacy when using email on behalf of the village.

1.1 Ownership of email

- All **email users** of village email accounts will acknowledge that they understand the village's policy on email ownership each time they log into the village's system.
- **Email users** who work at home (the village justice, historian, and board members) should have separate email accounts for village-related emails or, at minimum, should maintain village emails separately from personal emails.

1.2 Training

- The **village clerk** will ensure training on the email system for all new village officials and employees, and will also provide ongoing training, especially after upgrades or transitions to new email programs.
- **New employees** will not have access to and use of a village email account until they are trained on the village's email policies and procedures.

1.3 Policy review and updating

The records advisory board (which includes the village clerk, legal counsel, historian, and treasurer) will review this email policy periodically, especially if the email policy or management system described herein changes.

2. Managing Email

The village manages most email as general correspondence and follows the retention periods for general correspondence in the Records Retention and Disposition Schedule MU-1. The village manages and preserves emails with a retention period of longer than six years in a central file directory on the village's main server, and ensures email with a retention period of six years or less is destroyed after six years.

2.1 Classifying email

- **Email users are responsible** for classifying emails, on receipt or before transmission, as either not records or as permanent records. Non-records and permanent records are defined as follows:
  - Emails that are not records include listserv messages distributed to many recipients, spam, broadcast messages received by officials and employees, and personal messages. A user may destroy non-records immediately.
  - Permanent emails document significant policy, decision making, events, or legal issues, or pertain to legal precedents.
- Users must remove permanent emails from their individual email accounts and store them in the shared file directory on the village's main server.
- The village's email archiving appliance will capture all emails, including permanent emails, and will prevent modification or deletion of archived email.

2.2 Managing retention and disposition

- Permanent emails will be managed and preserved in the shared file directory, along with the village's other electronic records (see below under "Preservation").
- The **village clerk** will ensure that emails generated during a certain year are purged from the email archiving appliance after six years.
- **Email users** who work at home should create two subfolders for permanent and non-permanent (six-year) emails, and delete all non-records. They should then periodically forward the two subfolders to the **village clerk**, who will file the permanent emails in the shared file directory. It is not necessary for the clerk to manage the non-permanent emails, because the system will automatically collect the emails from the clerk's account and manage the emails as six-year records.
- In rare instances, **email users** may receive or send an email or attachment that either does not qualify as correspondence or that they wish to save for longer than six years but not permanently. In such cases, they must forward the email to the **village clerk**, who will apply the appropriate retention period and file the email in the shared directory. (**Users** of personal accounts should also follow this procedure.)
- The email server deletes all messages from individual accounts in the village email server after ninety days. (**Users** of personal accounts are strongly encouraged to purge these accounts of village-related email according to the same schedule, after forwarding copies of record emails to the village clerk as described above.)

- **Email users** may store non-permanent records that they need for daily use on their own computer hard drives. The **village clerk** will prompt email users to review files on their personal drives annually, and to delete those saved emails that have passed their legal retention periods.
- Destruction of emails on the archiving appliance may be halted under certain circumstances (see Section 4, "E-Discovery").

2.3 Backups

- The **village clerk** will ensure that backups of emails on the email server and the archiving appliance are destroyed according to the retention period stipulated for backups in the *Records Retention and Disposition Schedule MU-1.*

2.4 Preservation

- Emails with retention periods greater than six years will be preserved with other electronic files in the village's shared file directory.
- Emails will be stored in Rich Text format (.rtf) on the email archiving appliance and in the shared directory.
- Emails stored in the archiving appliance are compressed, but the vendor of the appliance has assured the village that the emails can be decompressed if needed without data loss (as documented in the village's contract with the vendor).
- The **village clerk**, with assistance from the **village's computer support vendor**, will monitor new versions of email software and the archiving appliance to determine whether upgrades are necessary.
- Backups of the email system and archive are to be used for disaster recovery purposes only, not for retention.
- The **village clerk**, with assistance from the **village's computer support vendor,** will ensure the ongoing integrity of media used to store emails, as stipulated in the Regulations of the Commissioner of Education (Part 185, *8NYCRR*), if the emails are moved offline to removable storage media.

3. Access to Email

Emails must be accessible for the duration of their retention periods. Emails are public records that are open and accessible to the public under the same conditions as all other village records.

- **Email users** have access to the emails in their individual accounts in the village system for ninety days. If they need access to some emails for longer than ninety days, they must save those emails on their personal hard drives.
- Permanent emails are filed in the directory first by village department and thereafter by subject or document type. **Users** have read-only access to

emails in the shared directory, with some important exceptions. Access to certain emails relating to ongoing law enforcement investigations, court actions, and personnel matters may be restricted by law to specific individuals in village government. The **village clerk** will maintain a list of types of emails where access is severely restricted.

- The **village clerk**, as records access officer, will respond to all FOIL requests involving email and, if necessary, will confer with legal counsel about an appropriate response (especially if a request is denied).

4. E-discovery

Village staff and officials must be aware that all email messages, including personal communications, may be subject to discovery proceedings in legal actions, and all must respond appropriately to an impending legal action involving email.

- **Legal counsel** will work with the village clerk to establish procedures for preserving evidence relating to imminent or ongoing legal actions.
- If a **village staff member or official** becomes aware of potential litigation, it is his or her responsibility to notify legal counsel immediately. Counsel will determine what action, if any, needs to be taken.
- **Legal counsel** will work with the presiding judge and opposing counsel to narrow the parameters of a records search as much as possible.
- The **village clerk**, working with the **village's computer support vendor**, will ensure that records of potential relevance in the archive remain accessible for the full extent of the proceeding, which may require moving relevant email records to removable storage media.
- All measures taken in response to an e-discovery action will apply to village-related emails that are retained by **email users** working on home computers.

5. Appropriate Use

Appropriate use will be handled as a security issue. Violation of the village's appropriate use policy can threaten the village's computer system, make the village vulnerable to legal action, and cause irreparable damage to the village's reputation.

5.1. Responsibility for appropriate use and system security

- All **email users** are expected to know the difference between appropriate and inappropriate use of email. This appropriate use policy applies to anyone who is representing the village, even if that person is using a personal account on a home computer.

- All users will be prompted to acknowledge their personal responsibility for using email appropriately every time they log into their village email accounts.

5.2 Inappropriate uses of email

Email is provided as a tool to assist **village employees and officials** in their day-to-day work, facilitating communication with each other, our constituency, and other stakeholders. The village email system is intended for official communications only, and it is everyone's responsibility to limit personal use of the system.

It is not acceptable to use the Village of Hidden Valley's email for

- any illegal purpose
- transmitting threatening, obscene, or harassing materials or messages
- distributing confidential village data and information
- interfering with or disrupting network users, services, or equipment
- private purposes, such as marketing or business transactions
- installing copyrighted software or computer files illegally
- promoting religious and political causes
- unauthorized not-for-profit business activities
- private advertising of products or services
- Modifying, obtaining, or seeking information about files or data belonging to other users, without explicit permission to do so

5.3 Enforcing appropriate use

- The village has the right to address instances of email misuse through disciplinary action or termination, if necessary. Messages relating to or in support of illegal activities must be reported to the appropriate authorities.
- The village clerk has access rights to all email on the archiving appliance to monitor and ensure system security.
- The village board will review alleged violations of the email appropriate use policy on a case-by-case basis.

6. Technical Security

The village's computer support vendor has primary responsibility for overseeing the technical security of the village's email management system.

- The **village's computer support vendor** is responsible for providing and maintaining up-to-date anti-virus software, firewalls, and spam filters to

protect the overall system from malicious email messages and other forms of sabotage.

- In the event that **email users** receive unsolicited email (spam) or email with unexpected and suspect attachments, they must delete these emails and report them to the village clerk, who will confer with the village's computer vendor to assess the security risk.
- **Users** should exercise similar care when linking to external websites from unsolicited messages.
- **Email users** must employ passwords to access their email in the village email system and must change their passwords periodically.
- As a general rule, **email users** must not share their passwords with other village officials or employees. In cases of planned or emergency absences, other personnel may be allowed to access the absent person's email, with prior approval from the **village clerk**.

7. Staff Departure

- If a staff member or official separates from the village, the **village clerk** will place a hold on the email account of that individual until the account and computer can be reviewed for record content.
- Any village emails maintained on a home computer by a former employee must be transferred to the **village clerk** for review and disposition.

8. Training

All village employees and officials will be trained in established email use and management policies.

Training will be provided to **all village email users** within the first ten days of employment or appointment, and to all employees when the policy is revised or the village changes its current email management system.

The **village clerk** will provide or arrange for training that will address the following topics:

- identifying records, permanent records, and general records management practices
- responsibilities of employees in records and email management
- costs to the village and the individual of not managing email
- use of the village email application and its relationship to non-system village email
- appropriate use of village email accounts

- responding to legal actions and FOIL requests

Training materials can also be obtained by contacting the village clerk.

Other Responsibilities

The person or persons responsible for certain functions associated with managing email are indicated throughout this email policy in boldface. Other responsible parties (and their respective responsibilities) are listed below.

1. Village mayor and village board

- ensure an adequate budget allowance for maintaining the email management system
- promote, support, and enforce this email policy
- review alleged violations of the email appropriate use policy on a case-by-case basis and adopt disciplinary measures as needed

2. Village counsel

- reviews and approves contracts with vendors to ensure they are consistent with village law and with the village's internal procurement practices

3. Village bookkeeper

- maintains an inventory of all computer hardware and software as part of the village's fixed assets inventory

4. Computer support vendor

- implements user profiles to allow village staff and officials to access the email and other records management applications

Sample Policy 2

Town of Big Thunder: Email Policies and Procedures

Effective October 2008

Email Management System Capabilities

Below are the capabilities of the management system maintained in town hall. The town also provides email accounts on the home computers of a small number of town officials who occasionally work at home. These accounts exist separately from the internal management system and do not have the following capabilities.

a. Captures the text, attachments, and transmission data of an email message.

b. Prompts individual users via a dialog checkbox (with three choices, as described under "Classifying Emails") to classify incoming and outgoing email messages before closing or sending the messages, and thus manages emails based on how users classify them.

c. Includes an archiving module for permanent and six-year records with an interface that mirrors the main email interface, to reduce the need for further training.

d. Stores permanent and six-year emails and their attachments in the email archive immediately upon receipt, replacing the actual file on an individual desktop with a stub file that links to the file in the email archive; deletes the archive pointers and short-term messages from the email system after sixty days, unless they are flagged for longer retention.

e. Saves only one instance of emails as they are moved to the central email repository and destroys the copies.

f. Prevents modification or deletion of archived email to ensure the town's email records are legally admissible in court. If a user forwards or replies to an archived email, the user creates a new email record.

g. Archives individual emails in a directory structure that is arranged according to different departments. Access to individual emails within a department or across the archives is primarily via a search engine.

h. Permits litigation holds that suspend destruction of those records (including backups) that may be relevant to an impending lawsuit.

1. General Policies

The town legally owns all emails that employees and officials create and receive in the process of conducting business on behalf of the town and its constituents. Employees and officials have no promise of personal privacy.

1.1 Ownership of email

All users of town email will be prompted to acknowledge that they understand this concept of ownership each time they log into the system.

Town officials and employees who do not have offices in a town facility or who must work after hours may sometimes conduct town business on home computers. These individuals must recognize that all town-related emails are public records that are covered by the *Records Retention and Disposition Schedule MU-1* and by this town email policy, and are subject to disclosure under FOIL, a court action, or an audit.

Town officials and employees who work at home should have a separate town email account on their own computer. They should periodically forward town-related emails to the town clerk in folders that reflect the classification system described below (see "Classifying Emails").

1.2 Roles and Responsibilities

The management of email is the responsibility of town officials at all levels and includes everyone who uses email to conduct town business.

Below are the individuals who have specific responsibilities for managing the town's email. These responsibilities are indicated throughout this policy under each main subject heading and are also listed at the end under "Summary of Responsibilities."

a. Town clerk, who is by law the town's records management officer (RMO), and who also functions as the records access officer

b. Town attorney, whose services are retained by the town under contract

c. Town supervisor and town board [or town council]

d. Town bookkeeper [or deputy town supervisor or other appropriate official]

e. Town IT director [or computer support vendor]

f. Records advisory board, whose members are currently the town clerk (as RMO), town historian, legal counsel, and bookkeeper

g. Email users, who can be anyone using email (including a town account on a home computer) to conduct business as a town staff member, elected official, or paid service provider. The town currently has approximately fifty email users.

1.3 Training

No employee will have use of a town email account without appropriate initial and ongoing training.

New employees will not have access to and use of a town email account until they are trained on the town's policies and procedures for managing email.

Ongoing training will be offered after upgrades, transitions to new email programs, and on an as-needed basis (at the request of an employee or if correction is required). See Section 10 for a description of the extent of our training program.

1.4 Policy review and updating

To ensure that this policy is current and relevant, it will be reviewed according to a set schedule and updated as needed.

The records advisory board will review this policy annually and modify it as needed to ensure that it is up to date.

The next review and revision of this policy will be in October 2009.

2. Maintaining the Email Management System

The technical maintenance of the system will be a coordinated effort involving several key players with defined roles and responsibilities.

2.1 Town supervisor and town board

a. ensures an adequate budget for maintaining the email management system

b. promotes, supports, and enforces this and other records management policies

2.2 Town clerk (as RMO)

a. ensures that appropriate state retention requirements are applied to all system documentation and associated records (use logs, group address books, master password register)

b. ensures that the current system and all future enhancements meet federal and state records requirements

2.3 Town IT director

a. maintains the technical capabilities of the email management system through scheduled upgrades and migration

b. implements user profiles to allow town officials and employees to access the email and other records management applications

2.4 Legal counsel

reviews and approves contracts with vendors to ensure they are consistent with town law and with the town's internal procurement practices.

2.5 Town bookkeeper

maintains an inventory of all computer hardware and software as part of the town's fixed assets inventory.

3. Classifying Emails

All email will be managed as correspondence according to a predetermined classification system. Users must classify email immediately on receipt or before transmission, and the system will automatically manage the email based on how the email is classified.

3.1 Classification system

Non-records
Email users are responsible for evaluating each email they receive to determine if it is or is not a record. Non-record emails are those that do not relate to the business or interests of this town. Non-records include listserv messages distributed to many recipients, spam, broadcast messages received by town officials and employees, and personal messages. A user may destroy non-record emails on receipt.

In addition, the town maintains a spam filter program that identifies and deletes all email that is presumably of a non-business nature, based on a combination of the sender name and address, keywords in the subject line, and the name of the attachment. Employees and officials have the opportunity to review filtered emails to determine whether any need to be restored, along with any attachments, to their mailboxes.

Email records
For email records, the town maintains an email management system that requires users to classify emails they send and receive through use of a dialog checkbox (with three choices) that appears when users try to send or close an email. The three categories that appear in the dialog checkbox are

a. Permanent: Emails that document significant policies, decision making, or events, or dealing with legal precedents or significant legal issues. The system will route permanent emails to the email archive and flag them for permanent retention.
b. General: Emails that contain legal, fiscal, or administrative information relating to town business; for example, those that initiate, authorize, or complete a town business transaction, and those that may be subject to a

fiscal audit. The system will transfer general business emails to the email archive and flag them with a retention period of six years.

c. Short-term: All of the emails listed below will be deleted from the system after sixty days unless they are deleted individually before that time.

   1. Emails having no informational, administrative, or fiscal value, such as transmittals, cover letters, invitations, and appointments
   2. Email records that are duplicates of official record copies. For example, if a recipient prints and files an email in a paper records system or stores a copy of that email on a shared network drive, that recipient may apply a shorter retention period to the email copy.
   3. Emails that are not records
   4. Individual emails that together constitute a continuous thread. The person who initiated the thread should classify the last email, containing all exchanges on the topic, as either permanent or general (six year) and the individual messages as appropriate for destruction after sixty days.

The categories above generally parallel the categories for correspondence indicated under item 10 in the State Archives' *Records Retention and Disposition Schedule MU-1.* The legal retention for emails with short-term fiscal, legal, or administrative value has been extended from "0 after no longer needed" to sixty days, for the convenience of email users.

Email users who use a town account on a home computer should create three subfolders that reflect the classification system above (Permanent, General, and Short-term). They should then periodically forward the folders to the town clerk, who will integrate the emails into the town's email management system.

In certain isolated instances, town officials and employees may receive or send emails that do not qualify as correspondence and therefore don't fit the three categories in the classification system. In such cases, they must forward these emails to the town clerk, who has the capability to override the classification system and apply retention periods other than permanent, six year, or sixty days, when appropriate. (Users of personal accounts should also follow this procedure.)

If a user receives an attachment with a retention period longer than the retention period of the message, the user must indicate in the checkbox the longer of the two periods.

The town clerk, as RMO, is responsible for working with staff and officials to clarify and provide ongoing training on which emails fall into each category and which emails may be exceptions to the classification system.

The records advisory board will periodically review the classification system to ensure that it reflects email use.

3.2 Compliance

The RMO, working with the town's technology vendor, will periodically audit the system to ensure users are classifying emails correctly. Those users who are not complying with the procedures will be required to undergo further training. If the problem persists, a user may lose his or her email privileges.

4. Access to Email

Access to email must be possible for the full retention period of the email but subject to strict controls to ensure against unauthorized or inappropriate access.

Users generally are limited to access to their own emails, unless they can demonstrate a need for access to the emails of another individual or department (for example, if they are working on a collaborative project or share a job function).

Email users have access to the emails in their individual accounts for sixty days, after which the emails will be purged. Users can continue accessing permanent and six-year emails that are older than sixty days in the email archive.

Users may file emails in their personal email accounts in any manner that is convenient to them. In the email archives, however, emails are filed first by department, and then by retention and disposition rather than by subject area or document type.

Town staff and officials must rely on a search engine to find individual emails.
To enhance searching, email users must assign intelligible subject lines to all outgoing emails. Users are encouraged to use consistent, meaningful terminology that mirrors file titles in the town's conventional paper filing system.

The town clerk, as RMO, and the IT director have access to all town email records in the email archive and can allow access to legal counsel and others on an as-needed basis. Access to certain emails relating to law enforcement investigations, court actions, and personnel matters may be restricted by law to specific individuals in town government. The town clerk will maintain a list of types of emails to which access must be restricted.

The town clerk, as records access officer, will respond to all FOIL requests involving email.

The IT director is responsible for ensuring access to email records for the duration of their retention periods.

5. Retention and Disposition

The system will manage the retention and disposition of sixty-day email automatically, and support the retention and disposition process for permanent and general emails. Certain circumstances (legal proceedings, FOIL request, audits, staff departures) will require that the town be prepared to suspend or supersede retention and disposition procedures.

5.1 Managing retention and disposition

The town clerk, as RMO, is responsible for advising on all retention and disposition issues associated with email, including the retention and destruction of backups.

Working with the RMO, the IT director ensures that appropriate technical measures are in place to preserve permanent and six-year emails (see "Preservation" section), destroy emails that have passed their retention periods, and halt the destruction of email, if needed.

Legal counsel is responsible for initiating the process of halting the destruction of records, including email and email system backups, in response to an impending legal case or some other need. Legal counsel must alert the town clerk (as RMO), who will contact the IT director to halt the destruction process.

Retention and disposition is tied to the town's classification system for email records, as indicated under Section 3, "Classifying Emails." Email users classify, and the system tags, emails as either permanent, general (six-year), or short-term (sixty-day) records when they receive or send an email.

The town clerk can apply a retention period that is not part of the classification system (permanent, six year, or sixty days) in isolated instances when appropriate.

5.2 Backups

The town creates backups of its email system as a disaster management strategy only. Backups are not intended to be archival copies of permanent records.

The *Records Retention and Disposition Schedule MU-1* indicates that system backups should be retained for three backup cycles. Retaining backups for longer than the defined retention period exposes the town to unnecessary risks in the form of lengthy records searches if the town is served with a court order.

5.3 Suspending retention

The town is aware of its legal obligation to suspend all retention and

disposition activities in the event of an impending lawsuit (see Section 6, "E-Discovery"). Emails may be retained once their retention periods have expired if needed for an impending or ongoing fiscal or program audit or a legal investigation.

5.4 Destruction

The system identifies the email records that must be destroyed after six years.

The IT director is responsible for destroying obsolete records, with prior approval from the town clerk. The current method of destruction is for the IT director to transfer records that have passed their retention periods onto CDs and arrange for the physical destruction of that storage media.

5.5 Staff Departure

If a staff member or official separates from the town, the town clerk must place a hold on the email account of that individual until the account and computer can be reviewed for record content.

This requirement may be waived when enough notice is provided in advance by the departing staff member so that the individual can appropriately deal with the records and is able to demonstrate this to the town clerk.

Any town emails maintained on a home computer by a former employee must be transferred to the town clerk for review and disposition.

6. E-discovery

Town staff and officials must be aware that all email messages, including personal communications, may be subject to discovery proceedings in legal actions, and all must know the appropriate response to an impending legal action.

Legal counsel will work with the town clerk (as RMO) to establish internal procedures for preserving evidence relating to imminent or ongoing legal actions. These procedures are subject to review by the town's records advisory board.

If a town staff member or official becomes aware of potential litigation, it is his or her responsibility to notify legal counsel immediately. The town attorney will determine what action, if any, needs to be taken.

Legal counsel will work with the presiding judge and opposing counsel to narrow the parameters of a records search as much as possible so as not to overburden the town's technical infrastructure.

In the event of an extended legal proceeding, the town clerk, working with the town's IT director, must ensure that records of potential relevance to the

case remain accessible for the full extent of the proceeding, which may require moving relevant email records offline to storage media or a detachable drive.

7. Appropriate Use

Appropriate use will be handled and enforced as a serious security issue. Violation of the town's appropriate use policy can threaten the town's computer system, make the town vulnerable to legal action, and cause irreparable damage to the town's reputation.

7.1 Responsibility for appropriate use and system security

All users of the town's email are expected to know the difference between appropriate and inappropriate use of email. This appropriate use policy applies to anyone who is sending or receiving email as a representative of the town, even if that person is using an account on a home computer.

All users will be prompted to acknowledge their personal responsibility for using email appropriately every time they log into their email accounts.

7.2 Inappropriate uses of email

Email is provided as a tool to assist town employees and officials in their day-to-day work, facilitating communication with each other, our constituency, and other stakeholders. It is intended for official communication only, and it is everyone's responsibility to limit personal use of the system.

It is not acceptable to use the Town of Big Thunder's email services for

a. activities unrelated to official assignments or job responsibilities
b. any illegal purpose
c. transmitting threatening, obscene, or harassing materials or messages
d. distributing confidential town data and information
e. interfering with or disrupting network users, services, or equipment
f. private purposes, such as marketing or business transactions
g. installing copyrighted software or computer files illegally
h. promoting religious and political causes
i. unauthorized not-for-profit business activities
j. private advertising of products or services
k. any activity meant to foster personal financial gain
l. modifying, obtaining, or seeking information about files or data that belong to other users, without explicit permission to do so

7.3 Enforcing appropriate use

The town has the right and responsibility to

a. log network use and monitor file server space utilization by users

b. limit the personal use of email and emphasize to users that they have no promise of personal privacy

c. restrict listserv membership to those listservs that are directly related to the job and the work of the town

d. post key points of acceptable use onscreen when users log on to the email system

e. add an automatic disclaimer with the basic principles of appropriate use at the end of all outgoing messages

f. make clear that misuse will be addressed through disciplinary action or termination, if necessary, and that messages relating to or in support of illegal activities will be reported to the appropriate authorities

The town clerk and IT director have universal access rights to all email so they can monitor and ensure system security.

The town governing board will review alleged violations of the email appropriate use policy on a case-by-case basis. Violations of the policy that are not promptly remedied may result in termination of Internet and email services for the person at fault.

8. Technical Security

The town's IT director has primary responsibility for overseeing the technical security of the town's email management system, but the security of the town's system requires the cooperation of all email users. Technical security is ensured through a system of controls that include anti-virus software, firewalls, filters, and passwords.

8.1 System security features

The IT director is responsible for providing and maintaining up-to-date anti-virus software, firewalls, spam filters, and logs to identify unusual activity and to protect the overall system from malicious email messages and other forms of sabotage.

8.2 Handling suspect emails

In the event that email users receive unsolicited email (spam) or email with unexpected and suspect attachments, they must delete these emails and report them to the town clerk, who will confer with the town's computer vendor to assess the security risk. Under no circumstances should users open

suspect email attachments. Users should exercise similar care when linking to external websites from unsolicited messages.

8.3 Reviewing filtered emails

Employees and officials have the opportunity to review filtered emails to see whether any should be restored to their mailboxes, along with any attachments. If work-related emails from the same source are consistently blocked, the user should contact the IT director to determine whether emails from that source can enter the user's account unimpeded.

8.4 Passwords

All users must use passwords to access their email. As a general rule, they must not share their passwords with other town officials or employees. In cases of planned or emergency absences, other personnel may be allowed to access the absent person's email, with prior approval from the town clerk.

Users will also be required to change their passwords periodically. The IT director will alert users when it is time to initiate the password change.

9. Preservation

Except where indicated the town will apply all preservation standards described in this section to both the permanent and general (six-year) email records, to ensure that even non-permanent records are accessible for their full retention periods in spite of rapidly changing technology.

9.1 Storing long-term email

As previously stated, end users will identify and isolate all records with a long-term retention period by indicating whether email records are permanent or general (six-year) before saving or closing messages.

The system will move permanent and six-year emails to the archiving server on receipt.

The IT director will ensure that email categorized as general is destroyed after six years and that permanent email is transferred from the email archive server onto temporary storage media after six years.

9.2 Software upgrades

The town clerk, with assistance from the IT director, will monitor new versions of email software to determine whether an upgrade is necessary, balancing the need to ensure accessibility for the full retention period against data loss that may occur with each data migration.

9.3 Format standard

The town has adopted XML as its long-term format standard for permanent and general (six-year) email records to ensure accessibility for the full retention period and to facilitate any future migrations.

9.4 Backups and long-term preservation

Backups of the email system are to be used for disaster recovery purposes only, for retention purposes. Data on backups are not indexed and are in a proprietary compression format, making it less likely that the data will be accessible long-term.

9.5 Media integrity

The town will ensure the ongoing integrity of media used to store long-term and permanent emails, as stipulated in the Regulations of the Commissioner of Education (Part 185, *8NYCRR*).

10. Training

All town employees and officials will be trained in established email use and management policies. Training will occur immediately after employment or appointment and thereafter on a regular basis.

Training will be provided within the first ten days of employment or appointment, to all employees on an annual basis, and when the policy is revised.

The town clerk (RMO) will provide or arrange for training that will cover the technical aspects of the email system and the records management responsibilities of email users.

Employees who do not attend ongoing email use and management training are at risk of forfeiting their email use privileges. Training will address the following topics:

a. Identifying records and general records management practices

b. Responsibilities of employees in records and email management

c. The costs to the town and the individual of not managing email

d. Use of the town email application

e. Appropriate use of their town email account

f. How to write and communicate effectively via email

g. Responding to legal actions and FOIL requests

Training materials can also be obtained by contacting the town clerk for a copy.

Summary of Responsibilities

1. Town clerk

a. ensures the maintenance of all necessary system documentation and associated records for the mandated retention period

b. ensures the current email management system and future enhancements meet federal and state records requirements

c. works with individual email users to clarify and provide ongoing training on classifying emails

d. periodically audits the system to ensure appropriate classification

e. allows access to emails in the email archives to legal counsel and others on an as-needed basis

f. responds to all FOIL requests involving email

g. advises on retention and disposition issues associated with email

h. ensures that records involved in a protracted legal case remain accessible for the full extent of the proceeding

2. Town supervisor and town board [or town council]

a. ensure an adequate budget for maintaining the email management system

b. promote, support, and enforce the email and other records management policies

c. review alleged violations of the email appropriate use policy on a case-by-case basis and adopt disciplinary measures as needed

3. Town attorney

a. reviews and approves contracts with vendors to ensure they are consistent with town law and with the town's internal procurement practices

b. initiates the process of halting the destruction of records in response to an impending legal case

c. works with the town clerk (as RMO) to establish internal procedures for preserving evidence relating to imminent or ongoing legal actions

d. works with the presiding judge and opposing counsel to define the parameters of a records search

4. Town bookkeeper [or deputy town clerk, or town manager]

a. maintains an inventory of all computer hardware and software as part of the town's fixed assets inventory

5. IT director

a. maintains the technical capabilities of the email management system through scheduled upgrades and migration

b. implements user profiles to allow town staff and officials to access the email and other records management applications

c. ensures access to email records for the duration of their retention period

d. ensures that appropriate technical measures are in place to preserve permanent and six-year emails, completely and appropriately destroys emails that have passed their retention periods, and halts the destruction of email, if needed

e. has primary responsibility for ensuring the technical security of the town's email management system

6. Records advisory board

a. reviews this policy annually and modifies it as needed to ensure that it is up to date

b. reviews the classification system to ensure that it continues to reflect actual email use

c. reviews procedures for responding to an e-discovery action

7. Email users

a. acknowledge they understand that the town owns all emails and that they have no expectation of personal privacy when using the system

b. will not use personal email accounts to conduct town business, except in emergencies or when they cannot access a town email account

c. classify email immediately on receipt or before transmission, identifying and deleting non-record emails and choosing one of three categories to assign to the email records

d. assign intelligible subject lines to all outgoing emails

e. notify legal counsel immediately on becoming aware of potential litigation that may involve email messages

f. know and acknowledge, each time they log in, the appropriate and inappropriate use of email

g. undergo training when beginning to work for the town and on an as-needed basis

Sample Policy 3

State Office of Administrative Support and Analysis:

Email Policies and Procedures

Effective October 2008

1. General Policy

Email is an information asset that is owned by the Office of Administrative Support and Analysis and therefore by the state and people of New York. As such, the agency is required to manage the email system appropriately and in a manner that is compliant with current laws and regulations. The management of email is the responsibility of everyone in the agency.

1.1 Purpose of this email policy

a. Ensure the efficient management of email is a continuing administrative function of this agency

b. Provide a clear legal basis for actions pertaining to email and a clear definition of who is responsible for each aspect of managing email

c. Protect the rights and assets of the public and taxpayers by maintaining accessible, secure email records

d. Ensure the systematic legal destruction of obsolete email records and preserve those emails that are permanent records

e. Provide information quickly and easily when needed internally and by the general public

f. Integrate email management into the agency's overall records management program

g. Allow for the efficient extraction and transfer of archival email records to the State Archives

1.2 Ownership of emails

All agency staff are advised that the emails they use in their daily work are not their personal property. Staff should have no expectation of personal privacy for any email messages they create, receive, and maintain on their agency email accounts. All users of the email system will be asked to sign a statement acknowledging their understanding of this concept of ownership when first assigned an email account.

1.3 Staff who telecommute or travel

All users must be aware that any business-related emails they create on personal email accounts are subject to disclosure under FOIL, a court action, or an audit.

Program unit managers who supervise an employee who works at home on a regular basis (because of reasonable accommodation, for example) must contact the IT unit to acquire an agency-owned laptop for that employee.

Similarly, staff who conduct official business when traveling on behalf of the agency must use an agency laptop or PDA for state business, or rely solely on web access to their email accounts.

The IT unit will assign and distribute laptops or PDAs as needed, ensure each assigned laptop has the appropriate security controls, and provide dial-in and wireless access for each employee using an agency laptop to conduct agency business.

1.4 Instant messaging (IM) and voicemail

Currently only field staff use instant messaging (IM), and these messages are captured in our email system. These policies and procedures apply to the captured messages, as they do to all email messages. If, at some point in the future, agency voicemails are recorded and captured in our email system (voicemail via Voice Over Internet Protocol technology), these policies and procedures will also apply to the captured voicemails.

1.5 Roles and Responsibilities

Listed below are the staff members who have specific responsibilities for managing email. These responsibilities are indicated throughout this policy under each subject area. A comprehensive "Summary of Responsibilities" comprises Section 12.

a. Records management officer (RMO), who is appointed pursuant to the Regulations of the Commissioner of Education and is the head of administrative services. The management of email is only one of the responsibilities the RMO has for coordinating the agency's records management program.

b. Records access officer, who works in the Office of Counsel and is designated pursuant to the Freedom of Information Law

c. Information security officer (ISO), who is appointed pursuant to CSCIC's *Information Security Policy*. The secure transmission and storage of email is only one of the responsibilities the ISO has for developing and overseeing information security operations. The ISO reports directly to the chief information officer (CIO).

d. Information technology (IT) staff

e. Program unit managers

f. Legal counsel

g. Records coordination committee, which consists of records liaisons from each program area. The director of information technology and the records access officer are ex-officio members of the committee.

h. Email user, who is anyone assigned an account on the agency's email server

i. State Archives, which eventually acquires legal and physical custody of the agency's archival email records

1.6 Training

No employee will receive an email account before undergoing training on the agency's policies and procedures for managing email. Training will also be offered after upgrades, transitions to new email programs, and on an as-needed basis (at the request of an employee or if correction is required). See Section 11 for a description of the extent of our training program.

1.7 Policy review and updating

The records coordination committee will review this policy annually and modify the policy as needed to ensure it is up to date.

This policy is scheduled for review and updating in August 2009.

2. The Email Management System

The Office of Administrative Support and Analysis has invested in an email management system that is a component of the agency's enterprise content management (ECM) system. The email system is designed to handle most aspects of managing email automatically.

2.1 System specifications

[Here a government or agency may indicate the name of the email program used, its relationship (if any) to other electronic systems, the geographic scope of the system, and any other physical or technical aspects of the email system that gives context to the email policies and procedures.]

2.2 System capabilities

a. Filters spam messages, providing users with a listing of filtered email for their review.

b. Captures instant messages sent and received by field officers, and has the capability to capture voicemail sent via Voice Over Internet Protocol.

c. Filters for suspect content (explicit or harassing language) according to a predefined list of terms or combinations of terms. Also identifies and filters messages sent to external recipients that may contain Social Security numbers or other confidential information.

d. Captures the text of the email message, attachments, and transmission data that identify the sender and recipients and the date and time the message was sent or received.

e. Files emails in a file directory structure with one to two file folder levels (by function/retention and document type), based on predetermined business rules for each program area. File folders are linked to retention periods in the classification system. For more detail, see "Classifying Email."

f. Stores all emails and their attachments in the ECM repository immediately on receipt, saving only one instance of emails in the repository and destroying the copies.

g. Associates an email and its respective attachment.

h. Provides secure levels of access (read-only or no access) down to the individual folder level in the repository, as appropriate.

i. Provides a directory structure and search engine for all emails to which a user is allowed access in the repository.

j. Prevents modification or deletion of emails once they are in the repository, to ensure their legal admissibility. If a user forwards or replies to an archived email, the user creates a new email record.

k. Prompts IT staff when email records are ready for destruction, based on how users have classified them. IT staff then confer with the RMO to verify the records have passed their official retention periods.

l. Includes a scrubbing application that is compliant with standards for secure data destruction established by the U.S. Department of Defense. Only staff in the IT unit can activate the scrubbing application, but only with prior approval from the RMO.

m. Permits litigation holds that suspend destruction of records (including backups) that may be relevant to an impending lawsuit.

n. Converts emails and attachments to XML while retaining the original message formats.

3. Maintaining the Email Management System

System maintenance requires the involvement and cooperation of many individual across the agency, including all users of the agency's email system.

3.1 Program unit managers

a. support the work of the RMO

b. ensure policy development and enforce compliance with policy

c. foster cooperation between program areas

d. ensure ongoing financial support for the technology, staffing, and staff training required to support a policy-based email program

3.2 Records management officer

a. works with the IT unit and the State Archives to address all necessary system documentation and associated records (use logs, group address books, master password register) in a records schedule

b. ensures that the current system and all future enhancements meet federal and state records requirements, including retention and disposition

c. works with the agency's staff development unit to ensure all staff are educated on the records management aspects of email

3.3 Information security officer (ISO)

a. works with IT unit staff to ensure all appropriate security controls are implemented and maintained

b. works with the agency's staff development unit to provide annual, mandatory training to all staff on their role in managing email appropriately to ensure the security of the agency's information assets.

c. monitors email use, reports to program managers about evidence of abuse, and administers corrective action to those staff members who are found to be misusing email

d. develops and maintains the agency's overall information security policy, of which email management is one component

3.4 Information technology (IT) unit staff

a. maintains the technical capabilities of the email management system through scheduled upgrades and migration

b. implements and maintains user profiles to allow staff to access email and other records management applications in the ECM

c. maintains an inventory of all computer hardware and software

d. provides technical training on how to use the email system

e. with approval from the RMO, implements the scrubbing application to destroy obsolete email records completely

3.5 Legal counsel

reviews and approves contracts with vendors to ensure they are consistent with the state's technology procurement practices, as outlined by the Office for Technology, and with the agency's records management and email policies

3.6 Email users

a. support the work of the RMO

b. attend records management, security, and technical training on email

c. classify all email promptly and appropriately

d. understand the policies relating to email and manage their own email accounts in accordance with those policies

e. report evidence of misuse or security breaches

4. Classifying Emails

The system will manage email according to business rules established during system design to reflect the use of email by individual program units and, in some instances, job functions. Users must classify email immediately on receipt or before transmission, and the system will manage the email based on how the email is classified.

4.1 Classification system

The system includes a spam filter program that identifies and deletes all emails that are of a non-business nature, based on a combination of the sender's name and address and keywords in the subject line and body of the email. Staff have the opportunity to review filtered emails to verify whether or not the emails are spam.

The system prompts individual users with a checkbox to classify incoming and outgoing email messages before closing or sending. The contents of the checkbox are customized for program unit areas that share the same function.

a. The checkbox has no more than five choices for the function of the email records; each choice in the checkbox is linked to a file folder in the repository's directory structure, which is, in turn, linked to a retention period in a State Archives' retention schedule.

b. The agency has worked with the State Archives to develop retentions based on function rather than on records series, to reduce the number of possible retention periods in a single program area.

c. One choice in the checkbox is "not record." Emails that are not records are those that do not pertain to the business or interests of this agency. Non-records include personal messages and listserv messages distributed to many recipients. If a user checks "not record," the system deletes that email.

d. Depending on the program unit to which a user belongs, the user's choice in the first checkbox may trigger a second checkbox indicating document type.

e. The system then automatically files records chronologically.

The RMO, working with individual records liaisons, will periodically review the classification system to ensure that it reflects email use and the appropriate retention periods for email in their program areas.

The records coordination committee will review and coordinate requests for changes to the classification system with IT staff.

4.2 Compliance

The RMO, working with the program unit liaisons and the IT director, will periodically audit the system to ensure users are classifying emails correctly. Those users who are not complying with the procedures will be required to undergo further training. If the problem persists, a user may be subject to disciplinary measures.

5. Access to Email

Access to email must be possible for the full retention of the email but is subject to strict controls to ensure against unauthorized or inappropriate access.

5.1 Internal access

Users generally have access to their own emails in the repository and to units with which they share a specific job-related function. They can access the emails of other departments if they demonstrate the need (for example, if they are working on a collaborative project). Access to emails in the repository is read-only.

Users can search through files of emails in the repository based on records function or use the repository's search engine. To enhance searching, email users must assign intelligible subject lines to all outgoing emails. Users are encouraged to use consistent, meaningful terminology that mirrors file titles in the agency's other filing systems.

The IT director and ISO have access to all agency email records in the repository, and can allow access to legal counsel and others on an as-needed basis. Access to certain emails relating to legal investigations, court actions, and

personnel matters may be restricted by law to specific individuals in the agency. The agency RMO will maintain a list of types of emails to which access must be severely restricted.

The IT unit is responsible for ensuring access to email records for the duration of their retention period.

5.2 Public access to emails

The agency provides public access to records in accordance with the New York State Freedom of Information Law (FOIL).

The records access officer will confer with the appropriate program unit and the IT director to prepare an appropriate, timely response to a FOIL request involving email.

FOIL requests received via email must be answered by email, if the agency has the ability to do so.

The records access officer will respond to a FOIL request within five business days. There are three responses the agency may make:

a. Make the emails available

b. Deny access in writing (citing the reasons for denial)

c. Furnish a written acknowledgment of receipt of the request and a statement of the approximate date when the request will be granted or denied

If a request for access is denied, an appeals procedure is available. If the RMO (as records access officer) intends to deny access, the RMO must consult with legal counsel to ensure that this is an appropriate response.

6. Retention and Disposition

The system will manage retention and disposition on a regular basis, according to the classification that users assign to emails. Certain circumstances (legal proceedings, FOIL requests, audits, staff departures) will require the agency to suspend or supersede standard retention and disposition practices.

6.1 Managing retention and disposition

The RMO is responsible for advising on all retention and disposition issues associated with email, including the retention and destruction of backups.

Working with the RMO, IT staff will ensure that appropriate technical measures are in place to preserve emails (see Section 10, "Preservation"), destroy emails that have passed their retention periods, and halt the destruction of email, if needed.

Working with the RMO, IT staff will identify, extract, and transfer archival email records to the State Archives.

Legal counsel is responsible for initiating the process of halting the destruction of records, including email and email system backups, in response to an impending legal case or some other need.

Email users are responsible for classifying emails appropriately, since the agency's classification system is tied to retention rules.

6.2 Backups

The agency creates backups of its email system as a disaster management strategy only. Backups are not intended to be preservation copies of permanent records.

The State Archives' general records retention schedule indicates that system backups should be retained for three backup cycles. Retaining backups for longer than the defined retention period exposes the agency to unnecessary risks in the form of lengthy records searches if the agency is served with a court order.

6.3 Suspending retention

The agency must suspend all retention and disposition activities in the event of an impending lawsuit (see Section 7, "E-Discovery"). Emails may also be retained once their retention periods have expired if needed for an impending or ongoing fiscal or program audit or legal investigation.

6.4 Destruction

The system alerts IT staff when records have passed their official retention periods and are ready for destruction. IT staff notify the RMO, who authorizes destruction after conferring with the appropriate program unit liaison.

IT staff implement destruction, using the system's scrubbing application for secure destruction.

6.5 Staff departure

If a staff member will be separating from the agency, that staff member's supervisor must notify IT to place a hold on the account until the staff member's email, computer, and (if field staff) any portable communications tools can be reviewed for record content.

This requirement may be waived when enough notice is provided by the departing employee so that the employee can appropriately dispense with his or her records and can demonstrate this to the program area supervisor.

7. E-discovery

Agency staff must be aware that all email messages, including personal communications, may be subject to discovery proceedings in legal actions. All staff must know the appropriate response to an impending legal action.

Legal counsel (who is also the records access officer) will work with the agency RMO to establish internal procedures for preserving evidence relating to imminent or ongoing legal actions. These procedures are subject to review by the agency's records coordination committee.

If an agency staff member becomes aware of potential litigation, it is his or her responsibility to notify legal counsel immediately. Legal counsel will determine what action, if any, needs to be taken.

Legal counsel will work with the presiding judge and opposing counsel to narrow the parameters of a records search involving emails as much as possible so as not to overburden the agency's technical infrastructure.

In the event of an extended legal proceeding, the RMO, working with IT, will ensure that records of potential relevance to the case remain accessible for the full extent of the proceeding, which may require moving relevant email records offline to storage media or a detachable drive.

8. Appropriate Use

Appropriate use is a security issue. Violation of the agency's appropriate use policy can threaten the agency's computer system, make the agency vulnerable to legal action, and cause irreparable damage to the agency's reputation.

8.1 Appropriate use and system security

All users of the agency's email are expected to know the difference between appropriate and inappropriate use of email.

All users must acknowledge their personal responsibility for using email appropriately as a part of their orientation into the agency and thereafter each time they log into the system.

8.2 Inappropriate uses of email

Email is provided as a tool to assist agency employees in their day-to-day work. It is intended for official communications only, and it is everyone's responsibility to limit personal use of the system.

Conversely, the use of personal email accounts and technology to conduct agency business is explicitly prohibited. Personal email accounts and equipment suspected of being utilized to conduct agency business may be subject

to search or seizure in the event of legal action that involves agency records.

It is not acceptable to use the agency email services for

a. activities unrelated to official assignments or job responsibilities
b. any illegal purpose
c. transmitting threatening, obscene, or harassing materials or messages
d. unauthorized distribution of agency data and information
e. interfering with or disrupting network users, services, or equipment
f. private purposes, such as marketing or business transactions
g. installing copyrighted software or computer files illegally
h. promoting religious and political causes
i. unauthorized not-for-profit business activities
j. private advertising of products or services
k. Modifying, copying, or seeking information about files or data belonging to other users, without explicit permission to do so

8.3 Enforcing appropriate use

The agency has the right and responsibility to

a. log network use and monitor file server space utilization by users
b. limit the personal use of email and emphasize to users that they should have no expectation of personal privacy
c. restrict listserv membership to those listservs that are directly related to the job and the work of the agency
d. add an automatic disclaimer with the basic principles of the agency's appropriate use policy at the end of all outgoing messages
e. make clear that misuse will be addressed through disciplinary action or termination, if necessary, and that messages relating to or in support of illegal activities must be reported to the appropriate authorities

The ISO and IT director have universal access rights to all email so they can monitor and ensure system security.

The agency's governing board will review alleged violations of the email appropriate use policy on a case-by-case basis. Violations of the policy that are not promptly remedied will result in termination of Internet and email services for the person at fault, and referral for disciplinary actions as appropriate.

8.4 Alternatives to email for work-related activities

Email is not appropriate for transmitting and documenting the following work-related activities:

a. Information on impending personnel actions, such as employee disciplinary matters and performance evaluations

b. Confidential information or information that can be used to breach personal privacy (such as Social Security numbers or medical information)

c. Information that may jeopardize facility security

d. Formal or official communications that merit a printed or electronic document because of their importance

In the above instances, staff are advised not to use email and, when needed, seek alternative forms of recordkeeping or create no unnecessary records. In addition, staff involved in cooperative projects may decide to use collaboration software or a shared directory rather than email to document and share information about that project.

9. Technical Security

The ISO and IT unit will work together to ensure the technical viability of the email management system, including providing training for and monitoring the use of all email users.

9.1 Staff training

The ISO has primary responsibility for formulating the agency's technical security policy and training staff about it. To provide effective training, the ISO will work with the agency's staff development unit.

9.2 System security controls

The IT unit works with the ISO to implement technical security measures for the agency's email management system. IT staff are responsible for providing and maintaining up-to-date anti-virus software, firewalls, spam filters, and intrusion detection logs to protect the overall system from malicious email messages and other forms of sabotage.

9.3 Handling suspect content

In the event that email users receive unsolicited email (spam) or email with unexpected and suspect attachments, they must delete the emails and report them to the ISO, who will confer with IT staff to assess the security risk. Under no circumstances should users open suspect email attachments.

Users must exercise similar care when linking to external websites from unsolicited messages.

9.4 Handling filtered email

Agency staff have the opportunity to review filtered emails to see whether any of them should be restored to their mailboxes, along with any attachments. If work-related emails from the same source are consistently blocked, the user should contact the IT unit to determine whether emails from that source can enter the user's account unimpeded.

9.5 Passwords

All users must use passwords to access their email. They must not share their passwords with anyone who works in the agency or with anyone outside the workplace.

The system will enforce the use of passwords for emails by prompting employees to change their passwords every six months. Employees who fail to change their passwords when prompted will lose access to their email accounts. Reinstatement of access privileges will be possible only by working with IT staff.

10. Preservation

The agency will apply all preservation standards described below to any records with a retention period of longer than three years to ensure that even the non-permanent records are accessible for their full retention period in spite of rapidly changing technology.

10.1 Software upgrades

IT staff will monitor new versions of email software to determine whether an upgrade is necessary, balancing the need to ensure accessibility for the full retention period against data loss that may occur with each data migration.

10.2 Format standard

The agency has adopted XML as its long-term format standard to ensure accessibility for the full retention period and to facilitate any future migrations. The system automatically creates a copy of each email in XML.

10.3 Backups and long-term preservation

Backups of the email system are to be used for disaster recovery purposes only, not for retention purposes. Data on backups are not indexed and are in a proprietary compression format, making it less likely that data will be accessible long-term.

10.4 Media integrity

Per regulations, IT staff will institute the following maintenance procedures for electronic media that contain permanent emails:

a. Verify the media are free of potentially damaging errors.

b. Rewind under constant tension all tapes at least every two years.

c. Annually test a three-percent statistical sample of all units of media to identify any loss of data and to discover and correct the causes of data loss.

d. Copy immediately onto new media any permanent or archival emails stored on media that contain a significant number of errors or show signs of physical degradation.

e Copy all permanent or archival emails onto new media before the media are expected to fail, and always before the media are ten years old.

f. Prepare external labels to identify each media unit, the name of the organizational unit responsible for the records, and the records title.

10.5 Transferring archival email records to the State Archives

The agency will request that State Archives staff appraise potentially archival records for possible transfer to the State Archives. Some email messages may be retained in the agency permanently for long-term administrative use, although they may not be archival. Prior to transferring the email records, the RMO will work with the State Archives to ensure that the records are stored on removable storage media and in formats that are consistent with State Archives standards.

11. Training

Training on the technical aspects of the email system, these email management policies, security, and appropriate use will be part of a new staff member's orientation and will thereafter be ongoing.

All agency employees will be trained on these email management policies within the first ten days of their employment and thereafter on an annual basis or whenever the policy is revised.

The RMO will provide or arrange for training that will cover the records management issues associated with email and the records management responsibilities of email users.

IT staff will ensure that all employees receive training on the technical capabilities of the email program.

The ISO will implement annual, mandatory training on system security, including the use of email and the Internet.

Employees who do not attend mandatory email use and management training are at risk of forfeiting their email use privileges. Training will

address the following topics:

a Identifying records and general records management practices

b. Responsibilities of employees in records and email management

c. The costs to the organization and the individual of not managing email

d. Use of the government email application

e. Appropriate use of their government email account

f. How to write and communicate effectively via email

g. Responding to legal actions and FOIL requests

Training materials will be made available on the agency's intranet site, and can also be obtained by contacting the agency's RMO for a copy.

12. Summary of Responsibilities

12.1 Records management officer (RMO)

a. works with the IT unit and the State Archives to address all necessary system documentation and associated records (use logs, group address books, master password register) in a records schedule

b. ensures that the current system and all future enhancements meet federal and state records requirements, including retention and disposition

c. works with the agency's staff development unit to ensure all staff are educated on the records management aspects of email

d. works with the program unit liaisons and the IT director to audit the system periodically and to ensure users are classifying emails correctly

e. advises on all retention and disposition issues associated with email, including the retention and destruction of backups

f. works with IT to identify, extract, and transfer archival records to the State Archives

g. approves destruction of obsolete records, after conferring with the appropriate program area liaison

12.2 Legal counsel

a. (as records access officer) confers with the appropriate program unit liaison and the IT director to prepare responses to FOIL requests within five business days

b. reviews and approves contracts with vendors to ensure they are consistent with the state's technology procurement practices, as outlined by the Office for Technology, and with the agency's records management and email policies

c. initiates the process of halting the destruction of emails in response to an impending legal case or some other need

d. works with the agency RMO to establish internal procedures for preserving evidence relating to imminent or ongoing legal actions

e. works with the presiding judge and opposing counsel to narrow the parameters of a records search involving emails as much as possible

12.3 Information security officer (ISO)

a. works with IT staff to ensure all appropriate security controls are implemented and maintained

b. provides annual mandatory training to all staff on their role in managing email appropriately to ensure the security of the agency's information assets

c. monitors email use and administers corrective action to those staff members who are found to be misusing email

d. develops and maintains the agency's overall information security policy, of which email management is one component

e. has universal access rights to all email, to monitor and ensure system security

12.4 Information technology (IT) staff

a. assign and distribute laptops as needed, ensure each assigned laptop has the appropriate security controls, and provide dial-in and wireless access to each employee using an agency laptop to conduct agency business.

b. maintain the technical capabilities of the email management system through scheduled upgrades and migration

c. implement and maintain user profiles to allow staff to access email and other records management applications in the ECM

d. maintain an inventory of all computer hardware and software

e. provide technical training on how to use the email system

f. ensure that appropriate technical measures are in place to preserve emails, completely and appropriately destroy emails that have passed their retention periods, and halt the destruction of email, if needed.

g. implement destruction of obsolete records, with approval from the RMO

h. work with the RMO to extract and transfer archival email records to the State Archives

i. ensure that records of potential relevance to a legal case remain accessible for the full extent of the proceeding

12.5 Program unit managers

a. must contact the IT unit to acquire an agency-owned laptop for employees who work at home or travel

b. support the work of the RMO

c. ensure policy development and enforce compliance with policy

d. foster cooperation between program areas

e. ensure ongoing financial support for the technology, staffing, and staff training required to support a policy-based email program

f. notify IT about an impending staff departure to review that staff member's email account for record content

12.6 Records coordination committee

a. reviews this policy annually and modifies the policy as needed to ensure it is up to date

b. reviews the classification system to ensure that it reflects email use in each program area

c. with IT staff, reviews and coordinates requests for changes to the classification system

d. reviews, updates, and approves procedures for responding to e-discovery

12.7 Email users

a. support the work of the RMO

b. attend records management, security, and technical training on email

c. apply policy relating to email and manage their own email accounts in accordance with that policy

d. report evidence of misuse or security breaches

e. classify incoming and outgoing email messages before closing or sending the messages

f. understand the difference between appropriate and inappropriate uses of email

g. acknowledge their personal responsibility for using email appropriately as a part of their orientation into the agency and thereafter when logging into the system.

h. implement security measures for their email accounts (such as the use of passwords), as outlined in policy

12.8 State Archives

a. appraises potentially archival email records, and acquires legal and physical custody of all archival email records

b. provides technical advice on all aspects of managing email records, including retention and disposition

Appendix: The Legal Framework

Arts and Cultural Affairs Law

The Arts and Cultural Affairs Law defines records and mandates how the records of state agencies and local governments in New York State must be managed. Regardless of physical characteristics or form, the law applies to records that are "made, produced, executed, or received" by a local government or state agency, legislature, or judiciary "pursuant to law or in connection with the transaction of public business."

By law, an email message—in spite of its unique characteristics and form—is a government record if it is produced for government business. The state effectively claims ownership of all emails that agencies, the legislature, and the judiciary create or receive on behalf of the state, and local governments similarly own the email records of local officials. The law does not distinguish between locations where a record is created and media where it ultimately resides. The law applies to government-related emails on any computer (personal computers, laptops, PDAs) and media (tapes, server, personal hard drive), regardless of whether the computer or media are publicly or privately owned.

The Arts and Cultural Affairs Law assigns responsibility for the oversight of state and local government records to the Commissioner of Education, who delegates that responsibility to the State Archives, an office of the State Education Department. In particular, the commissioner is charged with authorizing the appropriate retention and disposition of records and with promulgating regulations that further define the stipulations of the law. Excluded from the commissioner's oversight are court records and the records of the state legislature, New York City, municipal housing authorities, and select other offices and local governments.

Commissioner's Regulations

Part 185 of 8NYCRR (Regulations of the Commissioner of Education) pertains to managing records in local governments. Part 188 concerns state government records. The regulations mandate that local governments and state agencies ensure the following when managing electronic records:

- Include records retention and other requirements in system design.
- Ensure electronic records are usable for the full retention period. State agencies are additionally required to transfer archival electronic records to the State Archives in a usable and accessible format.
- Create and maintain metadata about electronic records (seven required metadata elements are listed).

- Create and store backup copies in a secure offsite facility (which for state agencies can be the State Records Center).
- Take steps to ensure media integrity (six steps are listed).

If local governments and state agencies create, disseminate, and maintain records as emails, they must apply the above regulatory requirements to those email records.

Cyber Security Policy P03-002

The New York State Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) has promulgated a statewide policy on information security (*Cyber Security Policy* P03-002) that addresses all "information assets" regardless of format, including email, that are created and maintained by "state entities." The policy is also mandatory for any "outsourced third parties who have access to or manage state entity information," including local governments that exchange information with state entities.

The Cyber Security Policy includes a section on Internet and email appropriate use, but many of the broad subject areas the policy addresses are also relevant to any discussion of email. These subjects include physical and environmental security, portable devices, wireless networks, access controls, and monitoring and compliance. The security policy is available on CSCIC's website.

Federal Rules of Civil Procedure

Enacted in December 2006, amendments to the Federal Rules of Civil Procedure apply to e-records relevant to federal cases. The amendments have already been adopted by several states, and it is expected that more states will follow. Although not adopted in New York, the amended Federal Rules at least bring new prominence to existing state legislation and regulations pertaining to records.

The Federal Rules emphasize the following components of an e-records management program:

- An e-records inventory, because under the new rules both parties are required to meet within 90 to 120 days of the beginning of an e-discovery action to review a list of potentially relevant e-records
- Retention schedules that are regularly implemented, to prove that potentially relevant records have been destroyed appropriately
- Staff training, because the control of many electronic records, especially email, depends on an individual user

Most importantly, an e-records program must be regulated by written policies and procedures. The existence of policy is especially important if a party in a lawsuit seeks "safe harbor," a provision in the rules that places a limit on the efforts a defendant must expend to locate or produce records. As yet untested by litigation, safe harbor is intended to protect a defendant who cannot retrieve electronic records in spite of all best efforts.

Freedom of Information Law (FOIL)

Email is a record as defined by New York's Freedom of Information Law (FOIL). This means that, as with other records, the public has the right to gain access to messages in an agency (defined as all local governments and state executive branch agencies) email system, except for those emails or portions of them that fall into the ten categories of records that are exempt from disclosure under FOIL. Emails relating to government business that are created and received on home computers are also subject to disclosure under FOIL.

FOIL requires each agency to designate a records access officer, who is responsible for receiving and responding to FOIL requests from the public, including requests for disclosure of email.

An amendment to FOIL enacted in 2006 states that "if an agency has the ability to receive requests for records from the public and transmit records by means of email, it will be required to do so," using forms consistent with the request form developed by the Committee on Open Government.

In 2008, FOIL was again amended to clarify issues that govern access to electronic records. In terms of managing email, the most significant FOIL amendments are the following:

- Section 87, part 5(b): No agencies shall enter into or renew a contract for the creation or maintenance of records if a contract would impair public inspection or copying.
- Section 89, part 3(a): An agency shall not deny a request on the basis that the request is voluminous or that locating or reviewing the requested records or providing the requested copies is burdensome because the agency lacks sufficient staff or on any other basis.
- Section 89, part 3(a): Any programming necessary to retrieve a record maintained in a computer storage system and to transfer that record to the medium requested...shall not be deemed to be the preparation or creation of a new record.
- Section 89, part 9: An agency in designing its information retrieval methods, whenever practicable and reasonable, shall do so in a manner that permits the segregation and retrieval of available items in order to provide maximum public access.

Given the frequency with which FOIL requests (and the courts) focus on email, local governments and state agencies should ensure that their email records are accessible and that the efficient retrieval of emails is a key result when selecting or designing an email management system. If a local government or state agency relies in part or completely on one or more service providers to manage email, the government or agency must have the ability to extract, redact, and export emails from the host's system that are relevant to FOIL requests, preferably with as little effort (and additional cost) as possible.

For more information about FOIL as it relates to email, contact the New York State Committee on Open Government.

99-039 cdc