File Management Policy Ideas

Sample Computer Usage Policy

The following wording can be considered by an organization that is considering developing a policy to guide organization members to appropriate usage of the organization's Internet-related resources. This policy is referenced from Polices about Using Computers and Networks.

"The (organization's) internal network is connected to the Internet. Everyone with computer access to the internal network has the ability access the Internet, including use of electronic mail and the World Wide Web. While the Internet is a great resource for our organization, it is the responsibility of each employee to use this resource responsibly and respectfully. It is assumed that the predominant use of these resources will be for work use, and that any personal use of electronic mail or the World Wide Web will be limited; never a priority over work matters. If an employee is found spending excessive time on personal use of these resources, this privilege may be revoked for that employee.

Electronic mail sent from the Institute should be treated the same as any other communication that is sent. All communications represent the (organization name) as a whole, and as such, should be written in a professional and appropriate manner. This also applies to any material that is published on the (organization name's) World Wide Website.

If there are any question regarding this policy, please contact _____."

Backup Policy

1.0 Overview

This policy defines the backup policy for computers within the organization which are expected to have their data backed up. These systems are typically servers but are not necessarily limited to servers. Servers expected to be backed up include the file server, the mail server, and the web server.

2.0 Purpose

This policy is designed to protect data in the organization to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

3.0 Scope

This policy applies to all equipment and data owned and operated by the organization.

4.0 Definitions

1. Backup - The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.
2. Archive - The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.
3. Restore - The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

5.0 Timing

Full backups are performed nightly on Monday, Tuesday, Wednesday, Thursday, and Friday. If for maintenance reasons, backups are not performed on Friday, they shall be done on Saturday or Sunday.

6.0 Tape Storage

There shall be a separate or set of tapes for each backup day including Monday, Tuesday, Wednesday, and Thursday. There shall be a separate or set of tapes for each Friday of the month such as Friday1, Friday2, etc. Backups performed on Friday or weekends shall be kept for one month and used again the next month on the applicable Friday. Backups performed Monday through Thursday shall be kept for one week and used again the following appropriate day of the week.

7.0 Tape Drive Cleaning

Tape drives shall be cleaned weekly and the cleaning tape shall be changed monthly.

8.0 Monthly Backups

Every month a monthly backup tape shall be made using the oldest backup tape or tape set from the tape sets.

9.0 Age of tapes

The date each tape was put into service shall be recorded on the tape. Tapes that have been used longer than six months shall be discarded and replaced with new tapes.

10.0 Responsibility

The IT department manager shall delegate a member of the IT department to perform regular backups. The delegated person shall develop a procedure for testing backups and test the ability to restore data from backups on a monthly basis.

11.0 Testing

The ability to restore data from backups shall be tested at least once per month.

12.0 Data Backed Up

Data to be backed up include the following information:

1. User data stored on the hard drive.
2. System state data
3. The registry

Systems to be backed up include but are not limited to:

1. File server
2. Mail server
3. Production web server
4. Production database server
5. Domain controllers
6. Test database server
7. Test web server

13.0 Archives

Archives are made at the end of every year in December. User account data associated with the file and mail servers are archived one month after they have left the organization.

14.0 Restoration

Users that need files restored must submit a request to the help desk. Include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

15.0 Tape Storage Locations

Offline tapes used for nightly backup shall be stored in an adjacent building in a fireproof safe. Monthly tapes shall be stored across town in our other facility in a fireproof safe.

This policy may contain descriptions about how various systems and types of systems are backed up such as Windows or UNIX systems.

Developing a Policy for Managing Email

Table of Contents

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 (PO3-002) 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 model 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