netgovern™

POLICY ELEMENTS & TEMPLATE

4 ELEMENTS TO ADDRESS WHEN CREATING COMPLIANT ARCHIVING POLICIES

www.netgovern.com

POLICY ELEMENTS

Without a doubt, email is the most widely used software application in any organization. It increases productivity and profitability via improved communication and knowledge sharing. However, there are also downsides associated with the growth of email including the exponential amount of sensitive information communicated and stored. Enforcing compliance and archiving policies protects organizations from security threats, data loss, litigation risks, and noncompliance. For policies to be enforced, they first have to be tailored to your organizational needs. Do you know where to start?

It is evident that in today's highly regulated business environment, having an email policy is no longer a nice-to-have guideline; it is a Must-Have Process. If you want to be sure that your organization is protected against litigation and security threats, or if you simply want to achieve compliance with the statutes governing your respective industry, you will need a strong policy foundation.

Your Policy dictates the operational requirements and rules of deployment that must be adhered to and creates the basic blueprint to cover important legal and compliance issues directly related to your end users such as:

- Corporate confidentiality leaks

- Incorrect use of email for existing internal processes

- Liability claims against the organization for inappropriate or malicious use

Most organizations already have some sort of email usage policy in place – it may be formal or informal, and it may also cover other areas related to IT such as general security and access controls. However, given the complexity of modern collaboration and messaging infrastructures, if you want to be sure that your organization is protected against litigation and security threats, and if you want to achieve compliance, you will need a strong policy foundation that is 100% dedicated to email and which combines Acceptable Usage Policies with Records Management Policies.

At a minimum, you will want to address the policy elements that follow.

1 RETENTION POLICY

The first step to creating a retention policy is identifying governance and regulatory requirements. What kind of information is useful and for how long? What kind of information should be kept to comply with laws and regulations and for which period of time? This policy is classified as an organizational policy and it identifies the retention and deletion requirements for email within the organization. If users are given the ability to delete messages, then the policy should provide a clear definition as to what constitutes a business record and what constitutes a transient record that may be deleted. You should also have measures in place for random audits and validation that the policy is being followed. Often, organizations already have an existing records management policy for paper documents. It is a good idea to extend the current policies to include electronic messages, but keep in mind that your policies for documents (or electronic files) may not always extend efficiently to electronic messages. The most important concern is that you have alignment between how your organization treats similar information types, regardless of if this information is preserved on paper, on file, or as an attachment in an email message.

2 DELETION POLICY

Unless you plan on keeping information in perpetuity, you will at some point wish to delete information when it is no longer valuable or when the regulatory requirements have been met. Your deletion policy, which in essence is more of an operational policy, should take into consideration all forms of the email messages, including corporate archives, private archives and backups of messages. A deletion policy is only as good as the procedures to purge all information from the environment and should include audit trails that can validate the destruction.

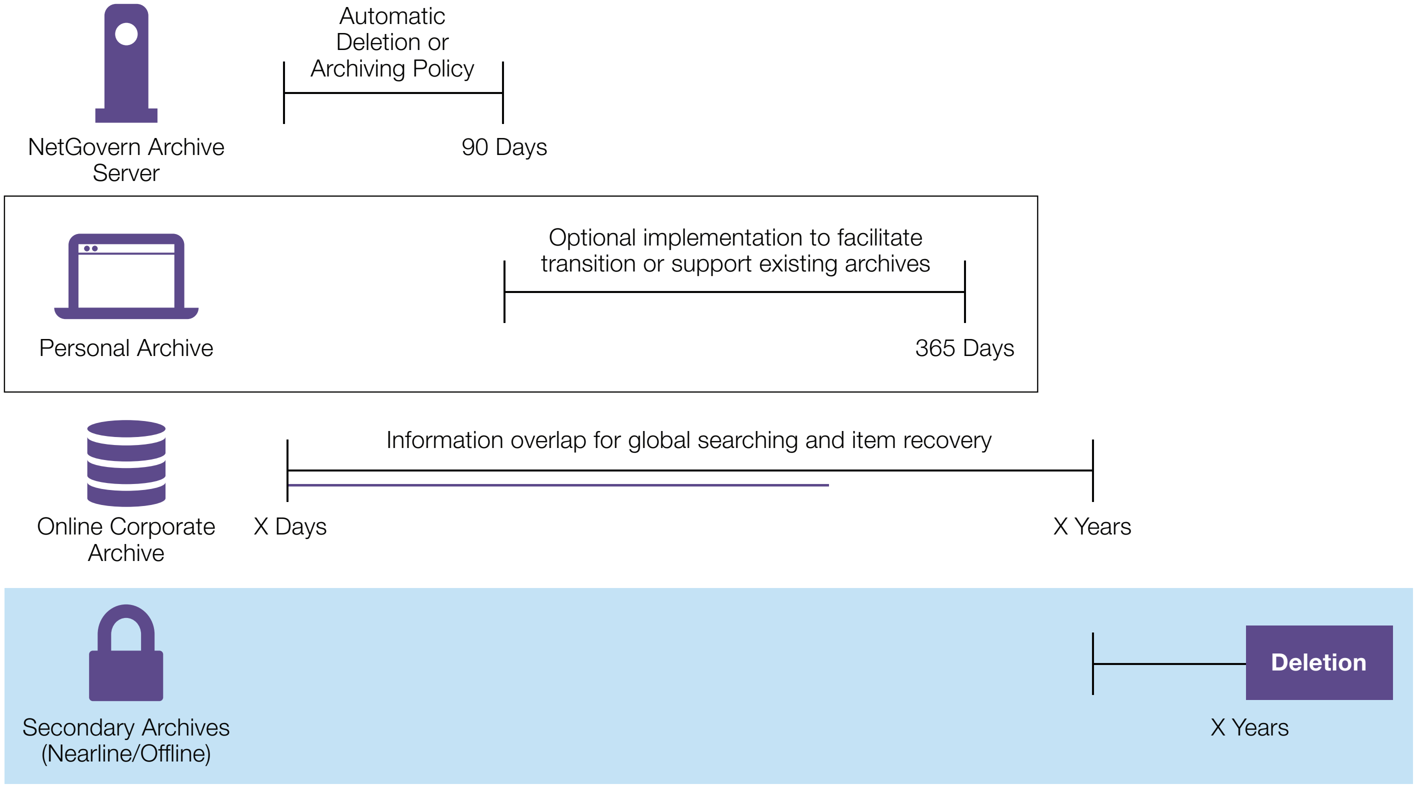
3 INFORMATION LIFECYCLE POLICY

This policy is critical to defining what data will be stored in your primary messaging systems, what data will be stored in online archive systems and what data will be stored in off-line systems. The policy needs to effectively communicate the use of corporate and private archives (i.e., personal archives will be allowed but not supported, or will altogether not be enabled), and the accessibility procedures for data not stored in online systems.

4 BACKUP POLICY

Many organizations still utilize tape backup for records retention, a practice that grew out of long cycle tape rotation, allowing administrators to recover a specific copy of a file quickly and easily. Unfortunately, since email is a database application, it does not afford this efficiency of storage and retrieval and backups actually prevent organizations from finding information rapidly.

EXAMPLE ARCHIVAL/RETENTION POLICY


NetGovern Archive Server
Automatic Deletion or Archiving Policy
90 Days
Personal Archive
Optional implementation to facilitate transition or support existing archives
365 Days
Online Corporate Archive
Information overlap for global searching and item recovery
X Days
X Years
Secondary Archives (Nearline/Offline)
Deletion
X Years

SAMPLE POLICY

On the following pages, you'll find a copy of the NetGovern Email Policy. Feel free to copy the content and adapt it to your organizational requirements. If you prefer to start from scratch, the key elements of your policy should include:

- Purpose of the policy
- Scope of the policy (who is affected by it)
- Explanation of what and how email is being monitored and manipulated
- Clear description of what is and what is not acceptable
- State what constitutes a breach
- Disciplinary procedure in cases of policy breach

It is useful to give each employee a pamphlet explaining what the email policy stipulates. The guide should not only clarify what is or is not deemed adequate, but it should also demonstrate the benefits of having a policy in place.

It is essential to receive employee support, agreement and acceptance of the policy. Employees should be educated about the policy to ensure that they understand it. State clearly the reasons for the action undertaken: to emphasize your point, perhaps cite recent court cases, productivity loss statistics and other relevant data. In addition, communicate the benefits to the employees and the business in the same way that you would sell the benefits of your product or service to your customers. It can also be beneficial to provide users with feedback on how the email policy is helping your business.

You need to remind employees (and inform new hires) of the email policy on a recurring basis. You can do this by sending the policy out via email each 6 months, by including it in your employee handbooks, holding seminars on the most effective ways of using email and reporting back on the benefits of having the policy in place.

NETGOVERN EMAIL POLICY

1 INTRODUCTION

This policy applies to all employees and associates of NetGovern and encompasses electronic messaging systems owned and supported by the company, instant messaging and Email capable mobile devices or smartphones. Combined, these elements are commonly referred to in this Policy as the Email System.

The purpose of this Policy is to ensure the proper use of our Email System and make users aware of what constitutes acceptable and unacceptable use. NetGovern may amend this policy from time to time – you will be informed of any changes. Failure to comply with this Policy may result in disciplinary action or sanctions and possibly the termination of your employment. You agree to abide by this Policy from the day you start your employment or association with NetGovern.

Reply to emailpolicy@netgovern.com, confirming that you have read and understood the contents. A copy of your email will be preserved as an official record.

2 SECURITY

Your Email account requires a username and confidential password. All users will maintain the security of their accounts by password protecting those accounts with secure passwords (minimum of 8 characters, alpha + numeric combination).

Do not share this information with anyone else at any time – you are responsible for the security of your account. IT Services will never require you to provide your Email username or password over the phone. All messages sent from your account will be deemed to have been created by you. If you believe that your Email account has been improperly accessed or tampered with, you must immediately advise IT Services (email address).

You should protect email messages, files, and records from unauthorized release to third parties. Suspicious demands for messages should be reported to IT Services Email messages sent to the outside world can be read by anyone monitoring our network or the intended recipient's network. You should not use Email to transmit sensitive or confidential information unless it is encrypted or in a password protected file.

If you own a mobile device or smartphone with email capabilities, it must have both power-on and idle timeout passwords enabled. If you use the device to access the company network or servers, you must not install unauthorized applications or alter security settings as these represent potential security risks. You must immediately notify IT Services in the event of the loss or theft of your device. NetGovern does not allow the use of Email services such as Hotmail, Yahoo or Gmail to conduct company business. These web sites may be blocked from access.

3 LEVEL OF SERVICE, USAGE, AND PRIVACY

The Email System allows delivery of messages both within the organization and to/from the Internet. This may include the use of proxy servers, forwarding rules, filters, gateways that may affect the delivery of certain messages to your account. Email message delivery to users outside the organization is not tracked and cannot be guaranteed.

We provide the Email System for the express purpose of facilitating the business of the organization.
Do **NOT** use it to:

- Send any content of inappropriate or discriminatory nature, even if as a joke.
- Send nuisance messages such as chain letters.
- Distribute messages or files not related to company business.
- For commercial purposes not sanctioned by.

Individuals using the Email System for personal use understand that the privacy and confidentiality policies outlined in this document apply to ALL messages. Any message is subject to review if stored on the company Email System.

Email messages sent to recipients outside of the company are may be intercepted and reviewed by software or services operating on the recipient's Email Servers. This may be conducted without our knowledge or permission.

4 CONTENT FILTERING

We scan the content of every email message that passes through our servers (inbound or outbound) based on predetermined criteria. If the message does not pass the criteria it will not be delivered.

Email message body and attachments are scanned for content that may contain specific words or expressions that are deemed inappropriate or represent a risk for the company. You will be notified if a message was not delivered and a copy of this message may be sent to the System Administrator for further review.

We restrict the receipt of virtually all executable files. These include but are not limited to files with extensions *.exe, *.com, *.bat, *.scr file types. All outbound excel spreadsheets will be blocked to avoid accidental transmission of sensitive financial data. All outgoing and incoming emails will be restricted to a maximum size of 50MB, to send files larger than this, you must use FTP. If your role requires that you be allowed to send or receive attachments that could be blocked, speak to your Manager or to IT Services.

5 MESSAGE RETENTION & DESTRUCTION

All email or electronic messages stored on or created on the Email System is the property of NetGovern and therefore are subject to retention. Mechanisms within the System guarantee 100% retention of all messages. These mechanisms do not allow the removal of any message or attachment from the Email System until a copy has been obtained and stored in the Archive.

The Company will retain all messages for a period of 7 years. Messages deemed transient or non-relevant, which you have stored in a designated folder will be purged from the archive after 1 year. However, messages may be retained for longer periods at the sole discretion of the company.

Contents of this archive are indexed and searchable. Like other forms of records, messages in the archive may be made public as part of internal audits, judicial or other public disclosure proceedings.

Personal archive folders are not supported and all personal archiving functions have been deactivated. All archived messages will be stored and accessed through the corporate archival system only. While backups of the Email System are conducted daily, these are considered “disaster recovery” only and not official message retention.

Automated destruction routines are run on a regular basis - archived messages will be destroyed at the term of their retention period in manner commensurate with proper disposal methodologies.

MESSAGING SYSTEM USAGE GUIDELINES

The following guidelines should be observed when composing or sending messages:

1 Avoid using all CAPS IN YOUR MESSAGES. This is regarded as shouting and can be considered angry or rude communication.

2 Be aware that emotions do not translate well in written form. Avoid any Internet chat abbreviations as many people will not understand.

3 Write well structured emails with an intuitive subject line, good sentence structure and no spelling mistakes.

4 Avoid replying to ALL when you are CC'ed or BCC'ed on a message. Being carbon copied is to keep you in the loop, if you were meant to be part of the discussion you would have been a primary recipient.

5 Avoid sending high priority messages unless truly urgent & important. You should not use distribution lists or message broadcasts except for making appropriate announcements.

6 Think before you send; messages composed too hastily or in anger can trigger terse arguments or bad feelings. Be aware that every message you send outside the company represents the company and that every message you send to your coworkers represents you.

ABOUT NETGOVERN

NetGovern's software enables regulated organizations to cost-effectively define and deploy vertical market ready Information Governance strategies in under 30 days, eliminating the "analysis-paralysis" phase that negatively impacts most enterprise data projects. Connect, Collect & Control petabytes of unstructured data stored in your file sharing, instant messaging, email and collaboration platforms, whether on-premise, on-cloud, or across hybrid systems. By providing comprehensive File Analysis (Audit), eDiscovery (Search), and Enforcement & Remediation capabilities, our clients can proactively organize, preserve, secure, and gain insight from what is arguably their most valuable asset – Information.

DO YOU NEED MORE GUIDANCE?

CONTACT US.

netgovern™

NetGovern, 180 Peel Street, Suite 333,
Montreal, QC H3C 2G7
514-392-9220 - info@netgovern.com