



Email Lifecycle Management Workbook

A guide to effective email control in Exchange and Outlook



Overview

This handbook can help you establish a Lifecycle Management strategy in your organization. Work through it and use it to help you formulate policy to: keep your email legal and lower your costs.

Email Lifecycle Management provides the professional messaging system administrator or manager with a framework to control the impact of email within the Exchange/Outlook environment. Effective Email Lifecycle Management minimizes the impact each item has on total system resources and reduces the legal risks associated with email.

Disclaimer of liability: While every precaution has been taken in the preparation of this document, C2C assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained herein.



Email Lifecycle Management

The lifecycle of an email runs from the moment it is first created, to the time when its last instance is permanently deleted from all electronic systems. This can range from a few seconds to months, or even years. Factors that determine the life span of an email include the end-user's attitude toward mailbox cleaning and filing, corporate e-Policy rules, industry regulations and messaging management technology.

During the lifecycle of an email, the messaging system administrator or manager needs to

- Minimize the impact of each and every email on the messaging system, to provide optimum system performance for all users
- Maintain fast access to all email, for both networked and remote users
- Monitor system security so email is safe from prying eyes
- Ensure each email can be searched should judicial/corporate requirements dictate
- Ensure each email can be appropriately archived and recovered for internal, legal or regulatory requirements

Three strategic areas are required to address these needs

Mailbox Size Management tackles issues of individual email item size, mailbox capacity and quota limits. Mailbox Size Management Strategy incorporates message size reduction, capacity management and optimized use of storage.

Search & Discovery tackles the issues of liability and security of email. This includes content searching, monitoring compliance with e-Policy, and mailbox and public folder access security.

Email Archiving considers the reasons for archiving: capacity, compliance and policy.

Checklist: User guidance

Problem: Users need direction on how to use an email system. They need guidelines on good and bad practice.

Solution: An e-policy should be a written statement from the company clearly defining what should and should not be done in the context of employment and corporate business. An effective email policy should contain:

- Clear statements on acceptable use of email
- Clear statements on unacceptable use of email in a personal context (e.g. racial, sexual, religious)
- Clear statements on unacceptable use of email in a corporate context (e.g. comment on business, competitors, applicable legislation, country laws)
- Statements on data retention (legal, regulatory)
- Comment on storage of personal emails
- Explanation of the impact of sending large emails
- Recommendations on the confidentiality of passwords
- Statements on enforcement actions that could be taken in case of deviation from e-policy



Checklist: Recommendations for improving and controlling mailbox size

Problems include: mailboxes becoming too large; running out of disk space; bandwidth issues; poor service; long restore times; retention of personal email; user frustration; productivity loss.

Administrator actions:

- Look at your users' mailbox statistics – categorize these as 'power user', 'normal user' and 'remote user' profiles
- Assess whether you need to control each group differently
- Decide whether the largest mailbox users need a targeted action plan to help them manage their capacity
- Create a capacity plan that goes beyond deletion of personal email – this only has a small impact on mailbox size
- Compare the benefits of automated (invisible) and non-automated data capacity tools
- Understand the benefits and implications of:
 - € Zipping/unzipping attachments at send/receive time
 - € Auto-zipping versus reliance on users
 - € Zipping attachments already in the message store
 - € Categorizing critical and non-critical data
 - € Removing less critical data to near-line storage
 - € Forced deletion of messages and/or attachments
 - € Creating roles for your servers
 - € Differing archiving strategies
- Set attachment compression standards if needed – what is a 'large' attachment?
- Produce a business plan for the user of compression and/or capacity management software. Estimate the measurable benefits (ROI) on employing data reduction technology for optimized use of bandwidth, remote data retrieval and disk storage. Ask software vendors whether they have a ROI estimate model
- Estimate benefits of zipping attachments at the Outlook client, OWA, Exchange server and gateway. Run automated capacity audits and warn users if they approach / reach limits
- Assess server recovery times, and their acceptability
- Every 60 days assess if the servers' capacity, growth and performance are in line with the initial design and deployment criteria, if not take remedial action
- Research the limitations of PSTs in your organization
- Understand the implications of a PST strategy in terms of data management, migration and storage. Assess whether archiving software can enact your corporate data policy
- Verify user impact of archiving email data against the user productivity. Ensure that remote mailbox access is considered in this review



Organization actions:

- Establish whether mailbox limits should be enforced at all, or whether business priorities should come first
- Establish where email stands in your total Disaster Recovery plan
- What is your SLA regarding email recovery?
- What are the corporate policies on document retention (time period, type of document)?
- Is there a deletion policy for some types of document, does it apply to email?
- Is email considered a company record?

C2C recommends:

MaX Compression from C2C automatically and invisibly zips and unzips email attachments sent and received across the Exchange system, therefore reducing email storage demands and network loadings.

Applications provide compression at the Outlook and Outlook Web Access clients, the SMTP Gateway and at the Exchange server, effectively reducing every email in the Exchange system to its optimal size.

Archive One for Policy from C2C can help to reduce mailbox size while enforcing a retention policy, moving emails to long-term storage selectively. Together, these tools can significantly reduce mailbox size and lower transmission, back-up and restore times.

Checklist: Recommendations for controlling and auditing exchange permissions and security

Problems include: Employees attempting to access confidential and sensitive information for personal interest or gain; security risk of changes to / mistakes in Outlook access permissions; need to run security audit of email and public folder access rights.

Administrator level actions:

- Discuss the implications of inadvertent/malicious access with your security team
- Communicate procedures if an employee accesses another's email
- Check the procedures in place for setting up mailboxes
- Check the procedures in place for deleting mailboxes and user permissions when an employee leaves your company
- Check the retention policy for former employee / leaver data
- Create rules to change passwords every 28 days (exclude any NT / Win 2000 service account password changes)
- Establish a list of those people who handle the most sensitive information
- Work with Security and give them the power to run security checks for you
- Run security checks on ALL mailboxes on a 90/180-day period
- Run security checks on VPs and Directors mailboxes at least every 30 days
- Construct a permissions matrix to validate the security check findings



- Make it corporate knowledge that permissions are monitored to help discourage the casual hacking attempt
- Remove global unrestricted Public Folder creation rights
- Establish a list of the most sensitive folders
- Run security checks on the most sensitive folders every 30 days
- Ensure User departments that have control of their own folders, understand the implications of permissions security
- Validate that Anonymous, Default and 'Zombie' permissions are managed correctly
- Understand the security implications of establishing remote mailbox access via OWA or RAS sessions
- Become familiar with the different types of Exchange permissions and the specific differences between different releases of Exchange

Organization level actions:

- Ensure that email security forms part of the corporate security plan
- Is email treated as a formal company record under corporate policy?
- Decide on enforcement or corrective policy for mailbox hacking

C2C recommends:

Archive One for Access Security Manager from C2C is an easy to use application for finding, auditing and changing Outlook folder and mailbox permissions that enhances the security of your Exchange System, by giving the Administrator the ability to review and change permissions quickly and accurately. Access Security Manager provides the means to audit large numbers of public folder and mailbox permissions to ensure system security, for both regular employees and the most security-sensitive email users, such as Human Resources.

Checklist: Reducing risk associated with email content

Problems Include: Vulnerability to risk of litigation due to inappropriate comment on colleagues, competitors etc.

Administrator level actions:

- Establish whose job it is to ensure that company email is used and retained within the law
- Ensure that your company directors and officers are aware of the issues associated with email content liability
- Provide your directors with recent stories regarding email misuse
- Establish how your organization could cope with a legal or internal request for a certain email
- Assess whether a frequent 'content audit' would reduce your organization's exposure to risk of litigation
- Review the tools required to enforce the e-policy and the manner in which they should be used

Organization level actions:

- Verify whether your company has a written e-policy regarding use and misuse of email
- It is most important to check that it is based on current regulation; some useful websites are listed in the 'What Next' section of this paper.



C2C recommends:

Archive One for Discovery scans 'live' Exchange Information stores and local or central PSTs for specific email content or attachment type, resulting in a lower risk of inappropriate use of organizational email. It can also be used as an additional anti-virus system, removing viruses before other software updates are available.

Checklist: Email Archiving, internal, legal and regulatory requirements

Problems include: Legal and regulatory requirements for retention, deletion and use of email differ by country, and often by state. It is essential that any organization, whether it is local or global in activity, understands and complies with requirements.

Organization level actions:

- Consult your internal or external legal advisors for advice on email policy
- Research your company records retention policy and whether it encompasses email
- Ensure that the solutions that you employ to control email are flexible and extensive enough to cover all requirements
- It is most important to check that it is based on current regulation for your country of origin and of potential trading

C2C recommends:

The C2C white paper "3 Reasons to Archive: Capacity, Compliance, Policy" can help you to select and develop an email archiving strategy that fits your organization. Download at www.c2c.com/site/downloads/download.asp.

What Next?

Sources of further information

- ePolicy Institute: <http://www.epolicyinstitute.com>
- Security Focus Online: <http://online.securityfocus.com>
- Electronic Privacy Information Centre: <http://www.epic.org>
- US: Securities and Exchange Commission: <http://www.sec.gov>
- US: Electronic Data Retention Policy: <http://www.sec.gov/divisions/corpfin/forms/exchange.shtml>
- US: Privacy Act: http://www.epic.org/privacy/laws/privacy_act.html
- US: Sarbanes-Oxley: <http://www.sarbanes-oxley.com>
- UK: Data Protection Act: <http://www.informationcommissioner.gov.uk>
- UK Companies Act: http://www.legislation.hmso.gov.uk/acts/acts1989/Ukpga_19890040_en_1.htm

The above list is not exhaustive; please seek legal advice for more detailed information.



About C2C

We hope that this paper has helped you to plan your way forward. C2C offers automated data archiving and management for email, files and SharePoint content. With over 15 years experience delivering solutions for capacity, e-policy enforcement, compliance and eDiscovery, C2C optimizes performance, reduces storage management costs and minimizes risks associated with email - helping you to control your data before it controls you.

The Company, a Microsoft Gold Certified Partner, supports organizations in the government, manufacturing, finance, education and healthcare industries, including Fortune 1000 companies. Established in 1992, C2C is a privately held company with offices in Springfield and Westborough, Mass. and Reading in the UK.

Copyright

All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. Disclaimer of liability: While every precaution has been taken in the preparation of this document, C2C assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained herein.

Where can I find out more?

For more information and free evaluation software, visit www.c2c.com or email info@c2c.com.

C2C Systems, Inc.
1 Federal Street
Bldg. 101-R
Springfield
MA 01105-1199
USA

C2C Systems Ltd
6 Richfield Place, Richfield Ave
Reading
Berkshire
RG1 8EQ
UK

T: +1 413-739-8575
F: +1 413-739-4980

T: +44 (0) 118 951 1211
F: +44 (0) 118 951 1111