

# E-mail Life Cycle Management Workbook

## Contents

<b>Page 3</b>	<b>Introduction</b>
<b>Page 4</b>	<b>Checklist: User guidance</b>
<b>Page 5</b>	<b>Checklist: Mailbox Size Management</b>
<b>Page 7</b>	<b>Checklist: Search &amp; Discovery - Permissions and Security</b>
<b>Page 9</b>	<b>Checklist: Search &amp; Discovery - Content Issues</b>
<b>Page 10</b>	<b>Checklist: E-mail Archiving- Internal, legal and regulatory</b>
<b>Page 11</b>	<b>Next Actions</b>
<b>Page 12</b>	<b>Appendix: sources of further information</b>

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

## E-mail Lifecycle Management: An Introduction

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

The lifecycle of an e-mail 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 e-mail include the end-user's attitude toward mailbox cleaning and filing, corporate ePolicy rules, industry regulations and messaging management technology.

During the lifecycle of an e-mail, the messaging system administrator or manager needs to

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

Three strategic areas are required to address these needs.

**Mailbox Size Management Strategy (MSMS)** - tackles issues of individual e-mail item size and mailbox capacity. MSMS incorporates message size reduction, capacity management and optimised use of storage.

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

**E-mail archiving strategy** – considers the reasons for archiving: Capacity, Compliance and Policy.

*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 e-mail legal and lower your costs.***

## Checklist: User Guidance

### **Problem:**

Users need direction on how to use an e-mail 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 e-mail policy should contain:**

- ❑ clear statements on acceptable use of e-mail.
- ❑ clear statements on unacceptable use of e-mail in a personal context (eg racial, sexual, political, religious).
- ❑ clear statements on unacceptable use of e-mail in a corporate context (eg comment on business, competitors, applicable legislation, country laws).
- ❑ statements on data retention (legal, regulatory).
- ❑ comment on storage of personal e-mails.
- ❑ explanation of the impact of sending large e-mails.
- ❑ recommendations on the confidentiality of passwords.
- ❑ statements on enforcement actions that could be taken in case of deviation from e-policy.

# Check list: 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 e-mail; 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 e-mail – 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 e-mail 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 e-mail stands in your total Disaster Recovery plan
- ❑ What is your SLA regarding e-mail 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 e-mail.
- ❑ Is e-mail considered a company record?

### **C2C Recommendations:**

[MaX Compression Enterprise](#) automatically and invisibly zips and unzips e-mail attachments sent and received across the Exchange system, therefore reducing e-mail 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 Capacity](#) is an e-mail archiving and capacity management solution to Exchange. A unique single technology solution, based within Exchange, it is fast to install and requires no adoption of other technologies. Archiving is controlled by advanced rules-based management and message retrieval remains transparent and immediate for the user.

[Archive One Policy](#) can help to reduce mailbox size while enforcing a retention policy, selectively moving emails to long-term storage.

**Together, these tools can significantly reduce mailbox size and lower transmission, back-up and restore times.**

# Check list: Recommendations for Controlling and Auditing Exchange/Outlook 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 e-mail 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 e-mail.
- ❑ 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 Exchange 5.5, 2000 and 2003.

**Organization level actions:**

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

**C2C Recommendations:**

[Exchange Security Risk Auditor](#) (ESRA) is an easy-to-use application for finding, auditing and changing Outlook folder and mailbox permissions. The objective of ESRA is to enhance the security of your Exchange System, by giving the Administrator the ability to review and change permissions quickly and accurately. ESRA 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 e-mail users, such as Finance or Human Resources executives.

# Checklist: Reducing Risk Associated with E-mail 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 e-mail is used and retained within the law.
- ❑ Ensure that your company directors and officers are aware of the issues associated with e-mail content liability.
- ❑ Provide your directors with recent stories regarding e-mail misuse.
- ❑ Establish how your organization could cope with a legal or internal request for a certain e-mail/s.
- ❑ Assess whether a frequent 'content audit' would reduce your organization's exposure to risk of litigation etc.
- ❑ 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 e-mail.
- ❑ It is most important to check that it is based on current regulation. Some useful websites to find out more are listed in the Appendix. This list is not exhaustive; please seek legal advice for more accurate information.

## C2C Recommendations:

[Active Folders™ Content Manager](#) scans Exchange Information stores and local or central PSTs for specific e-mail content or attachment type, resulting in a lower risk of inappropriate use of organizational e-mail. 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 e-mail 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 e-mail policy.
- ❑ Research your company records retention policy and whether it encompasses e-mail.
- ❑ Ensure that the solutions that you employ to control e-mail 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.

Some useful websites to find out more are listed in the Appendix.

### C2C Recommendations:

The C2C white paper “3 Reasons to Archive: Capacity, Compliance, Policy” can help you to select and develop an mail archiving strategy that fits your organization. Download at <http://www.c2c.com/3r.htm>

Archive One is a family of products that resolves the major email archiving needs:

- meeting retention regulations: [Compliance](#).
- improving system performance: [Capacity](#).
- enforcing e-Policy while improving system performance: [Policy](#)

## What Next?

We hope that this workbook has guided you to an overall view of your organization's preparedness for control of your Exchange system.

Can C2C help you to control your Exchange environment?

C2C has provided solutions to 2000 global organizations that use Exchange and over 3 million users. Our products and expertise can resolve the issues described earlier. Please contact us or visit our website [www.c2c.com](http://www.c2c.com)

## E-mail Life Cycle Management

E-mail Lifecycle Management					
Mailbox Size Management		Email Archiving Solutions		Search & Discovery	
MaX Compression Enterprise	Archive One Capacity	Archive One Policy	Archive One Compliance	Active Folders Content Manager	Exchange Security Risk Auditor

C2C Systems Inc.  
1 Federal Street  
Springfield Enterprise Center  
Springfield, MA 01105 USA  
T: 413-739-8575  
F: 413-739-4980  
info@c2c.com

C2C Systems Ltd.  
6 Richfield Place  
Reading, Berks  
UK RG1 8EQ  
T : +44 118 951 1211  
F: +44 118 951 1111  
info@c2c.com

**Free 30 day evaluation of products at**  
<http://www.c2c.com/download/default.asp>

## Appendix

### *Sources of further information:*

ePolicy Institute

<http://www.epolicyinstitute.com/>

Security Focus Online

<http://online.securityfocus.com/>

Electronic Privacy Information Center

<http://www.epic.org/>

UK: Data Protection Act:

<http://www.informationcommissioner.gov.uk/>

<http://www.hmso.gov.uk/acts/acts2000/20000036.htm>

UK Companies Act

[http://www.legislation.hmso.gov.uk/acts/acts1989/Ukpga\\_19890040\\_en\\_1.htm](http://www.legislation.hmso.gov.uk/acts/acts1989/Ukpga_19890040_en_1.htm)

UK: Regulation of Investigatory Powers Act 2000

<http://www.legislation.hmso.gov.uk/acts/acts2000/20000023.htm>

US: Securities and Exchange Commission

<http://www.sec.gov/>

<http://www.sec.gov/divisions/corpfin/forms/exchange.shtml>

US: Electronic Data Retention Policy

<http://www.lawresearch.com/>

US: Privacy Act

[http://www.epic.org/privacy/laws/privacy\\_act.html](http://www.epic.org/privacy/laws/privacy_act.html)

US: Sarbanes-Oxley

<http://www.sarbanes-oxley.com/>

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

Copyright © C2C Systems 2004.

All product and company names herein may be trademarks of their respective owners.