The Disconnect Between Legal and IT Teams

Sample Email Policy

#3 in a series of 4 whitepapers.

Circulate this document to IT, Legal, and company management.

It can be used to start a dialog, get consensus, and get action taken.

This whitepaper is published by Waterford Technologies, Inc., makers of the popular MailMeter archiving solution. For more information on MailMeter, email archiving, retention policies, ediscovery, FRCP, compliance, etc. go to www.MailMeter.com.

MailMeter

WATERFORD TECHNOLOGIES

Background

If your organization has still not made a decision to archive emails for business and legal purposes (FRCP, SEC, FINRA, and other regulatory or compliance purposes) or you are frozen (or still debating) in the decision cycle (keep everything vs. don't keep anything), then this whitepaper is for you.

Our goal is to provide understanding of both the legal and IT issues and offer ideas and suggestions to resolve the differences while meeting your business goals and mitigating the risks.

Over 80% of an organization's business intelligence is in email records.

Sales commitments, discounts, change orders, PO corrections, shipping changes, cost overruns, late deliveries, price changes, back orders, purchases, legal document changes, confidential information, etc. are transported through email.

The Disconnect

- Lawyers are worried about saving emails in an archive since they are discoverable records. Nearly every legal action includes an order to produce relevant emails.
- When your organization is aware that "there is good potential for a legal action" (even before they have been served with a subpoena) you must take formal actions to preserve any records that may be called as evidence or asked for in discovery. This includes notifying people not to destroy email records and tracking responses to the notices (litigation hold).
- The Federal Rules for Civil Procedure mandate that attorneys "Meet and Confer" to establish the "what do you have and where is it" for all electronic records expected to be searched.
- Your organization's users believe they need to save every email they ever sent or received forever (just in case).
- The IT team has to maintain backups and is tasked with making most ediscovery searches – which is time consuming, potentially expensive, and has a large potential for errors.
- Legal holds may require that copies of current mailboxes and messages on backups need to be recovered and placed in a separate, protected location.
- While the policy debate goes on, the mass of messages in the email server continue to grow and cause long backup times, potential for longer recovery times, and reduce reliability. IT is overwhelmed with storage costs, backups, and limited budgets.

Sample Email Policy

1. Introduction.

This policy is created to ensure that employees maximize the benefits of email usage and to minimize potential liability created by its use. All users of the email system are obligated to use this resource responsibly, professionally, and ethically.

2. General Statement of Policy.

Employees are given access to our organization's email system to assist them in performing their jobs. Email enables us to communicate promptly and efficiently with each other and enables us to deliver prompt and efficient service to our clients/customers/suppliers. Email can also be used to communicate with other individuals and businesses that we interact with.

While email brings many benefits to us in terms of its communications internally and externally, it also brings risks to our organization particularly where employees use it outside of their business roles. For that reason it is necessary to have a code of practice which regulates its use and which sets down its specific rules for the use of email.

The **email system and all messages and attachments sent or received are the property of our organization** and may only be used for business purposes, with limited availability for personal use.

Every employee has a responsibility to maintain the company's image, to use email in a productive manner and to avoid placing the company at risk for legal liability based on their use.

3. Monitoring.

All employees should be aware that all email and attachments that are sent or received are monitored, collected, and remain the property of the organization.

Employees **should not expect any measure of privacy** in emails that they send or receive. Every email may be subject to legal ediscovery or regulatory disclosure. Emails sent to government organizations are most likely accessible by the public under the Freedom of Information Act.

Without notice, any email can be reviewed by supervisory personnel for any reason including enforcement of rules and standards on email content.

4. Employee Use of Email

Email is a vital communication medium for our organization. It replaces and bypasses many printed forms of communications – changes to terms and conditions, quantities of items ordered, meeting schedules, and confirmation of decisions.

Each employee must realize and accept that there are *many risks with using email*:

- Your **message may go to persons other than the intended recipient** – by your error in entering and email address, by the email software "typing ahead" an incorrect name, or even by the recipient forwarding the email to someone else. If the message content is confidential or commercially sensitive this could result in damages to our organization or termination of your employment.
- Employees should use **extreme caution when sending confidential** information. Each email should be clearly marked as CONFIDENTIAL and include our standard confidential information and disclaimer addition to the message body.
- Email **messages can carry computer viruses**. Although we protect our email system with commercial anti-virus software, no assumption that every email is 100% virus free should be expected. Each employee should realize that visiting some internet web sites may cause viruses to infect their PC and be attached to email sent out or automatically generate infected messages to everyone in their address book.
- Caution must be taken in attaching letters, files, pictures, and other documents to any email if they were not generated by an employee. Those items may belong to others and have **copyright implications** in sending or receiving them without written permission. When in doubt – don't send potentially copyright protected materials.
- Email may **legally bind** our organization contractually in certain circumstances. Be careful – a simple "ok" can be a legal contract. Make sure you obtain proper authority for any potential contract change or agreement.
- **Do not send any email with personal information** about yourself or others. There are strict protection laws on use of social security numbers, credit card numbers, patient information, etc.
- **Deleting an email does not remove it from our archive.** Copies of all emails sent and received are kept as permanent records in a separate system.

5. Best Practices

- Write well structured emails that are clear, concise and communicate your intended message as briefly as possible.
- Use a short, descriptive Subject line. If possible, include a categorization – ACTION_NEEDED, NOREPLY, DONOTFORWARD, INFO_ONLY to make it easier for the recipient to organize their Inbox.
- Do not CC: a large amount of people. Everyone is burdened by the ever growing amount of email messages.
- Do not send unnecessary attachments. It wastes space in your mailbox and on our email server.
- Please spell check your messages. Use short abbreviations or acronyms to pass information quickly. Realize your recipient has other work to do.
- Be reasonable in the amount of newsletters and alerts that you subscribe to. You can be overwhelmed with the amount of "free" information sent to you and the need to keep up. Set up rules in your email client to move messages to READ folders automatically so you can process them at a convenient time.
- Your emails sent to persons outside our organization should include our standard disclaimer which states that this email is intended for the recipient only for business purpose and if received by any other person it should be returned to the sender.
- DO NOT USE CAPITALIZED WORDS in email messages. In email culture this means you are shouting or yelling.
- Only mark emails as urgent if they are really urgent and need response. Remember, not everyone is sitting in their email client – they may be on the telephone, in a meeting, out of the office, or working on another project.
- If you have sent and replied to an email more than 3 times, it is a good idea to pick up the telephone to complete a conversation.
- Do not use email as an instant messaging system. Industry studies show that emails take about 90 seconds to read and decide what to do. Emails also interrupt the normal thought process in a work task – writing a report, doing research, etc. In the past ten years email message volume has increased by a factor of 10. This means every email that is not a good business message, is an interruption that is costly to the recipient.
- Clean up your mailbox. Try to touch messages only once - take action, file for future reading, reply, or delete. Empty your Deleted Items folder. Purge

messages older than 1 year (91% of messages are read only once). Get rid of old email in your Inbox. Big mailboxes cause problems.

- If you receive an email that has inappropriate material – jokes, pictures, cartoons, language, hurtful remarks – sexist, racist, age, ethnicity, etc., please notify your manager or the IT department immediately.
- If you receive an email confirming a contract or agreement, it should be printed and included with the contracts, invoices, etc. files.
- Emails sent to persons not in our organization should have a signature section containing your name, title, organization name, address, telephone, and email address. Do not be creative with colors, font, and logos.
- Do not forward any email that says "Do not forward" or "Confidential".

6. Employees Should Be Cautious When Sending Email

- Be very careful when sending any confidential or commercially sensitive information in an email. Remember your emails may be forwarded to others without your consent. If you have concerns, please consult your manager.
- Do not send emails with disparaging remarks or that may be hurtful to others. Avoid the use of indecent, obscene, sexist, racist, or other inappropriate remarks whether it is written, cartoons, or pictures. Our organization does not tolerate any discrimination or harassment of anyone.
- Be aware of your emotional state when writing emails. If you are angry, you may inadvertently use language that is inappropriate or hurtful. An email should be considered a formal letter to the recipients – with the knowledge that a wider audience – managers, legal, media, new people it is forwarded to, etc. may see or publish a copy. Any indecent or indirect innuendo can have serious consequences for you and your employment.
- Do not send emails with large attachments. They clog up our email server and network bandwidth. They may also be refused by your intended recipient's email server (many organizations have a limit as to the maximum size of an email message and attachments).
- Each employee is accountable for their own actions in use of email. Keep in mind that any email you send, even to your best friend, could end up on the news and be used as evidence in a courtroom.
- If you use words such as "free" in your subject or messages to persons outside our organization, your email may be blocked by spam filters.

7. Prohibited Activities

- Sending, receiving, downloading, displaying, printing, or otherwise disseminating material that is sexually explicit, profane, obscene, harassing, fraudulent, racially offensive, defamatory, or otherwise unlawful.
- Sending or receiving messages for commercial activities (such as Ebay sales or real estate) that are not part of our business. Any activity for personal gain or profit is not allowed.
- Sending email to advance your personal political causes.
- Sending or receiving proprietary materials and confidential information of another party without their written permission.
- Sending viruses or phishing messages to anyone.
- Wasting email resources by sending mass emails, chain letters, etc.
- Violating any state, federal or international law.
- Forging or spoofing email messages, disguising your identity, representing yourself as someone else, sending email messages from another user's email account without their permission.
- Advertising or supporting unapproved or illegal activities.
- Sending email that contains proprietary material (for example customer or prospect lists), classified information, materials and information received under non-disclosure, or information obtained without permission.
- Spending unreasonable and unwarranted time on non-business email activities.

8. Breach of Email Rules and Policies

- Any breach of these rules will be treated seriously and will subject to disciplinary action up to and including termination, and civil or criminal liability.
- Employees having knowledge of any unauthorized email activities should report it to their supervisor.

9. Employee Notification of our Email Policies

- Each employee should be notified annually and required to verify that they have read and acknowledge the email policy.

Ideas and Suggestions

An email archiving solution brings value for legal, IT, and the business.

- Employees know that every email sent or received is kept as a company record for 7 years or longer. This insures that employees know not to waste resources on personal or frivolous mail.
- It prevents obvious use of the organization's email for non-business use since employees realize that every message is saved automatically.
- **Litigation hold is easy**. IT marks the message in the archive. No notices to users are needed. No user can delete messages in the archive.
- When email is reviewed internally, it is marked or "tagged" as privileged, needs review, responsive, case #, etc. and it remains with the message so future legal discovery is less expensive since messages have already been reviewed.
- Any ediscovery action can now be satisfied with internal staff who do the searches requested, review and mark the messages (big cost reduction), and export only the relevant emails to PSTs to hand to outside counsel.
- **Outside counsel costs are lowered**. There are significantly less emails to review. The litigator is familiar with the archiving solution and knows the searches produce all relevant email messages (nothing can be deleted by users from the archive). The meet and confer sessions go smoothly.
- Their need for business intelligence is satisfied – any user or manager can search the archive by date, keywords, customer, or person to find any critical email. The "needle in the haystack" can be found in seconds.
- IT is happy since email messages in the email server are removed after one year. Backups are smaller and recovery is easier. No more running out of disk space.
- **Depositions are easy**. A simple declaration of a description of the system and procedures usually suffices.
- **Retention management is absolutely controlled**. Messages can be destroyed by department, age, subject, person, content, etc.

Circulate this document to IT, Legal, and company management. It can be used to start a dialog, get consensus, and get action taken.

Message to legal

- Stop delaying a decision. It will only get worse in IT and create more legal problems (*read the blogs on the Guidance Software case*). Data is getting lost or destroyed and you haven't taken any actions to reduce your legal costs.
- Email archiving systems are not that expensive. In our experience the reduction in legal review costs on your first discovery action pays for the cost of the software.
- **Protect the business** – start collecting information now. You can always change your data destruction policies. Remember, you have anarchy now – people are making their own decisions. If you have a reduction in force, you may have lost years of good messages that can save you money in the future.
- **Be proactive** – head off litigation. With an eDiscovery tool you can do early case assessment in minutes, and can quickly decide if a case has merit.

Message to Business People

- **Protect the business** – start collecting information now. You are losing valuable data because people are wasting time managing to mailbox quotas (what should I save?) or sending valuable data outside the company to personal email accounts (and you don't know it).
- You can also improve productivity by letting users know you will keep everything so they can find it if they need it. No more dragging and dropping messages into folders or wasting time housekeeping to meet mailbox quotas (that's why executives have bigger mailboxes).
- Audit or sample emails – watch for the word "discount", "guarantee", etc. with an automated process to identify potential risk areas.
- Analyze email activity by department, domain, to give managers insight into their team's activities and help them manage better.

Message to IT

- Lawyers are not bad people. They have a tough job. They look to you to provide the insight into how to meet obligations without huge expenses. They will probably want IT to make the investment in email archiving because they are struggling with more cases and less money.
- Do them a favor – have them sit in on a non-technical demo of an email discovery solution. It will help.