

Email Compliance

A simple five-step guide by Trevor Williams

Techne-Comm Director



With 26 billion e-mails whizzing round the world in any one day (excluding spam), and the numbers going up, e-mail compliance is a matter that many companies often put on the 'back burner'. The consequences of this approach can result in litigation, financial penalties, HR problems as well as damage to company reputation. Corporate governance requires organisations retain their records for a specific period of time, which by default includes e-mails. Although much legislation pre-dates the Internet the regulations relating to e-mail are subject to the same ones as paper documents.

With many regulatory requirements being unearthed such as Sarbanes-Oxley, the Data Protection Act (European Union), Freedom of Information Act (UK) etc that often contradict each other, this article aims to shed some light on this area and provide you with five basic rules for e-mail compliance that will protect you from potential litigation, whilst at the same time provide you with some user benefits. Effective e-mail compliance does not have to be expensive and with data storage costs currently in the region of £1 per gigabyte the hardware costs are affordable.

The first rule is to take responsibility for archiving e-mails away from the user. There are two reasons for this, firstly the e-mail could be edited by the user before it's archived and is therefore not an 'original': secondly people resist change, so don't burden them with the decision making process of selecting which e-mail is important and which one is not. The best policy is to simply automate the whole process and capture all inbound e-mails before they ever reach user mailboxes and for sent items, as they are being transmitted. This ensures that they have not been edited or changed and you can guarantee the accuracy of content, timing etc of the e-mail when you are called upon to produce it i.e. it's forensically sound. Any e-mail compliance system should enable Systems Administrators to set up rules to exclude certain types of e-mails from the compliance archive because they are immaterial to the business or organisation e.g. Dilbert Cartoons, BBC News items etc and these exceptions must be auditable (see rule number four below).

It is good business practice to automatically archive e-mails away from your Mail Server or user Mailboxes to another separate system e.g. use a SQL database with a pointer to a separate data folder for the e-mails. The benefit of the SQL database approach is that the archiving process is completely separated from your Mail Server so if one or the other crashes then all is not lost. SQL database will also give you fast access when searching, finding and retrieving archived e-mails as well as easier backup and restore processes.

Rule number two, ensure that the archived e-mails cannot be changed or deleted. By using compression and encryption no alterations can be made and a forensically sound copy can be produced, in the e-mail's original format, when retrieved from the compliance archive. This is particularly important in legal situations, because you must be able to produce the original e-mail and not one that could have or had been edited in any way.

The third rule is to enable any e-mail or group of e-mails to be easily and quickly found and viewed from the compliance database. You need to be able to search on things that you are likely to remember for example a date range, part of an e-mail address, words or phrases in the text or subject line as well as specific data such as Contract Number, Invoice Number etc. Having constructed a search you then need to be able to refine the results by then 'searching within results'. It's pointless having an e-mail compliance archive if you cannot get to the e-mails you want to view quickly and easily.

By using a SQL database for archiving all e-mails then common index fields can be used to 'tag' or index e-mails so that members of the same group with a shared interest or responsibility can have access to all e-mails. This





will need user involvement in selecting and 'tagging' e-mails but the benefits of working with common index fields and getting away from personal folders far outweighs the time and effort involved.

Personally I believe that it's important to be able to retrieve copies of e-mails from the compliance archive back into the user's mailbox if it's an old e-mail that requires some action, with the original still remaining in the compliance archive. Many users save e-mails to their own private mailbox either on their local 'C' drive or on their mailbox server 'just in case I might need it some day'. The amount of storage they need grows and grows because they never clear out any 'dead' e-mails often taking up several gigabyte of disk storage per user.

A more pragmatic approach would be to encourage users to only keep current and 'active topic' e-mails in their own private mailboxes and delete 'dead' e-mails. If they ever needed an 'old' or 'dead' e-mail then the user can easily and quickly recover it from the compliance archive. This process will save considerable amounts of user disk storage space, help with user disk quotas as well as improving the performance of the Mail server.

Rule number four, ensure that the whole e-mail compliance process is auditable. Log files and counts need to be maintained as evidential proof of all actions taken relating to the e-mail compliance archive. Log files must prove that no e-mails can bypass the e-mail capturing process. Any or all compliance archived e-mails can then be searched for, found and viewed in their original format together with attachments.

Rule number five, advise your users that you have an e-mail compliance archive which captures all incoming and outgoing e-mails irrespective of whether they are internal or external. Tell them that they can access the e-mail compliance archive to find and view any e-mail and that they have access rights to e.g. their name is shown as the 'From' or 'To' or CC'ed or BCC'ed or they are part of a group that has been set up in Active Directory (they cannot see e-mails that they are not entitled to view).

In adopting an 'open' policy, users will be aware that Systems Administrators or similarly privileged users can view all or any e-mails together with attachments in the e-mail compliance data base and this awareness can act as a deterrent to e-mail abuse. Disciplinary action for new technology related offences (e-mail and internet abuse) now exceeds the combined total for dishonesty, violence and health and safety breaches according to the Chartered Institute of Personnel and Development. A survey by Integralis also revealed that 32% of Fortune 1000 companies have discovered employees passing confidential information to a third party.

Compliance is increasingly critical to the way in which businesses operate and by applying the above five rules you will be going a long way to taming the e-mail compliance sleeping tiger and putting a large tick in the e-mail compliance box. Ignoring e-mail compliance now could result in expensive and time consuming costs in the future. Remember e-mail compliance need not be costly, it should run seamlessly in the background improving day to day operations, and not inhibiting them.

About Techne-Comm

Founded in 1998, Techne-Comm is a software house offering a suite of affordable Windows based products in the area of electronic document management and archiving. As a dedicated supplier in this market it boasts an unrivalled technical knowledge and commitment to customer service in delivering document archiving and retrieval application solutions to businesses of all sizes. Its product range covers Web Archiver, FlickThru, ePost Room and the recently launched MailS@fe. Key clients include Three Valleys Water, Weber Saint-Gobain and Cambridge County Council.

For further information visit www.techne-comm.co.uk or www.mail-safe.co.uk

