Virya Technologies

ETHICAL TECHNOLOGY SOLUTIONS

White Paper: The Importance of a good Document Retention Policy

Introduction

Most businesses will create and rely on hundreds if not thousands of documents every year. We all recognise the importance of retaining these documents until we can be sure they are no longer required, but what of the other resources we use?

You probably ensure that you retain quotes and invoices raised, but what about email correspondence? Many will simply 'clear' their inbox when it starts to become overcrowded, but this could prove to be a huge mistake.

It's as important for employees to retain correspondence as it is for their employer. Documents may relate to communications with a prospective client or even simple notification of a sickness absence. Many would be forgiven for believing that the latter can be deleted once it has been read, but what happens in the future?

If you haven't retained documentary evidence, how will you defend your business if it is attacked? This could be in the form of a disgruntled client, making claims about an 'agreement' you reached or could be an employee accusing you of failing in your duty of care whilst they were ill.

As well as you may remember the period in question, the burden of proof in any such action is "on the balance of probabilities". That is to say, if a court or tribunal believes that your accusers version of events seems more likely to have occurred, you will lose - potentially at great cost to your business. This is why documentary evidence is so very important, but it will only be available if you've retained that evidence.

This paper will examine how we can retain that, possibly crucial, evidence and how a stringent retention policy will not only protect your business but also ensure that retention is not the mammoth task that it may at first seem.

Email

No-one likes having an overly full mailbox, and it would be ridiculous to suggest that users be required not to delete anything for a specific period of time.

Instead emails can be exported from the mailbox for filing in one of the manners we'll discuss later.

The easiest way to export an email from Microsoft Outlook is to open it and select File -> Save As->Document Type HTML. See below for a guide to exporting emails from Google Mail.

Your electronic working practices policy should specify the format of the filename, but the most practical is usually YYYYMMDD-Doctype_Description-Author.filenameextension
So an email sent 19 Jul 2011 about an outstanding order might be exported to 20110719_Email_Outstanding_order_from_supplier_X-BTasker.html

This filename format ensures that all documents will be displayed in chronological order by default. If you send multiple emails that day simply append a number to the date, so 20110719 becomes 20110719_1_ etc.

Traditional Documents

The more traditional types of document might include notes from a conversation, quotes, invoices and reports. It's highly likely that you already opt to retain most of these, but again the filename is very important if you wish to be able to locate it quickly in the future.

Your Electronic Working Practices policy should define the filenaming convention, but as with emails the recommended format is YYYYMMDD-Doctype_Description-Author.filenameextension. You can define the appropriate values for Doctype, but these may be "CallNotes", "Report", "Invoice" etc.

Paper or Electronic

So how should we retain and manage these documents? Many businesses will already retain a copy of some documents on paper, however there's no reason for it to be "either or". The space and administrative burden involved in storing everything on paper means that you should only retain a 'hardcopy' of those documents which absolutely require it.

However, there's no reason you can't digitise documents that you don't already have electronically. Consider investing in a scanner and ensure your staff scan documents when they receive them (a scanner with an automatic document feeder is highly recommended). This will lessen the burden of digitising documents as it will help prevent a backlog.

So, we now have a collection of electronic documents to retain. We're not particularly likely to want to store these in a single folder, so it may be wise to look into a document filing system. This could be as simple as a dedicated network share with appropriately labelled folders or a more advanced web-based system such as Sharepoint Team Sites (allowing for searching of documents).

How you categorise your documents will depend on your business, but don't make the mistake of categorising them by type. Ensure that each category relates to an aspect of your business (whether that be clients, employee's etc.).

Protect your Investment

Regardless of the financial cost (or lack thereof) you will have invested time and effort into document retention. It's therefore very important that you protect this investment and don't allow it to become a risk to your business in it's own right.

The most important thing to remember is: ***Only allow access to necessary areas***. If you are retaining any information relating to employees or customers you need to ensure that only those with authority can access these documents. Your employee's are likely to be less than impressed if their colleagues can view emails they sent you in confidence, and your customers will be far from happy if their data is leaked.

You can help ensure the security of this data by utilising encryption and managing user-access rights carefully. For example, It's likely that your employees will need to access customer information but shouldn't be granted access to data relating to your other employees. Design your system with this in mind.

Protect the integrity of your data - No matter what you retain, it'll be of no use to your business if it is lost. Ensure you run *regular* backups of your document retention system and if encryption is being used maintain a copy of the decryption key in a (*very*) secure location.

Designing your Retention Policy

A good retention policy specifies three things;

1. What should be retained
2. How it should be retained
3. The Retention Period

The latter two options are likely to vary depending on what is being retained. Whilst financial records may need to be retained for ten years, some businesses may think it less essential to maintain employee correspondence (sickness notifications etc.) for so long.

What - Your policy needs to identify the types of information that may need to be retained and then specify exactly how it should be retained (i.e. for contracts you may specify both electronically and in 'hardcopy') and for what period (i.e. the length of the contract + 5 years).

There's no need to be overly specific unless you can identify a direct business need, in most cases it should be sufficient to state 'contracts' rather than 'contracts with company B'.

It is important that you understand the difference that certain types of document could make to your business. As discussed earlier, if an employee were to take your business to an industrial tribunal claiming you failed in your duty of care to them, copies of emails sent and received could be absolutely invaluable. Even if the employee has copies, they may not admit to it (depending on their motivation), so it is essential that you retain evidence relating to any conversation that may be pertinent.

This also carries a benefit for your employee's, if a period of absence is queried long after the absence took place, it could be difficult for them to show that the absence was authorised and notified. If your document retention policy includes emails from that period it could help prevent a prolonged and stressful investigation.

How - Whilst it's obviously important to define how the documents should be filed, you also need to consider the format they should be stored in. For example, if a document has been created in a word processor, it may be wise to store this in a format such as Adobe's PDF to ensure that it cannot easily be edited in the future.

You may also find that you can strive towards an 'electronic by default' policy. For example, depending on your business you may benefit from the use of electronic signatures on contracts.

As you should only be filing 'finished' documents, it's important to consider ways in which you can reduce the likelihood of tampering or at least make said tampering easier to detect. Certain documents may need to remain read/write but many may benefit from a read-only format.

Retention Period - As important as it is to retain these documents, it's also very important to set a limit on how long they are retained for. This not only prevents the unnecessary build up of files, but also helps reduce the likelihood of someone deleting a document because they don't think it's needed any more.

A well specified retention period ensures that documents should be available for the period in which they may be required, as well as providing adequate explanation should a file be required once it has been deleted.

Try to keep retention periods as simple as possible, again to avoid inadvertent deletion of required files. This can be achieved by specifying the period following a specific date (i.e. 5 years after the end of the relevant financial year).

Even if you've specified multiple types of document to be retained, try and keep the number of differing retention periods to a minimum (i.e. 5 years, 7 years and 10 years). Again this will help to avoid confusion over the period which applies and prevent accidental deletion of files you may still need. Keep in mind, however, that you should not retain personally identifying information (customer account details, employee records etc.) for any longer than is reasonably necessary.

Conclusion

A good document retention policy is essential to every business, especially as society appears to grow ever more litigious. Failure to retain a document that is later needed could prove very costly to your business, so always err on the side of caution when deciding which documents to retain (especially as electronic storage grows cheaper by the day).

Once your retention policy is in place, ensure you protect the data carefully. Take steps to prevent unauthorised access to sensitive data, up to and including encryption. Regularly back the data up, as neither a court or tribunal is likely to see “our hard drive failed” as anything more than a convenient excuse as to why you can’t disprove an opposing parties claims.

Ensure that your policy is well thought out and doesn’t confuse your employees. An overly complicated policy could lead to documents being misfiled, or worse deleted erroneously by a confused user. Your businesses retention policy is your responsibility and don’t expect a court or tribunal to view this in any other manner!

Once your policy has been designed and implemented, your employees should soon become used to using it and business critical documents should be available if and when you require them in the future.

About the Author

Ben Tasker is an IT Manager & Linux Specialist at Virya Technologies. He has substantial experience within the IT Industry, and a keen interest in Network security.

More white papers and free resources available at http://www.viryatechnologies.com/

Advice for users of Google Apps

The cloud presents many benefits, and although at first glance it appears to make document retention a little more difficult, it simply introduces an additional step.

Here we'll examine the steps needed to create retain-able copies of emails and documents from within Gmail and Google Docs respectively.

- **GMail**

If you access your email through the GoogleMail interface, you don't have the option to simply File->Save As in the way that you do with Outlook. However, you can achieve similar results just as easily once you have installed some (free) software.

First we need to install a PDF printer, software such as BullzipPDF Printer is freely available and creates a 'printer' on your system that simply creates a file in Adobe PDF format.

Once this is installed, exporting from GMail is incredibly simple;

1. Open the email you wish to export
2. Click the down arrow in the top right hand corner of the email (next to Reply)
3. Select Print
4. When the print dialog appears, select the PDF Printer and press Print
5. You will be prompted to enter the filename of the document to create
6. Click OK

The email has now been exported to a PDF file and can be filed within your system.

- **Google Docs**

Exporting from Google Docs doesn't require a PDF printer, and you can export into multiple formats (for documents that won't require editing, PDF may be the best option). For this example we'll download the document as a PDF;

1. Open the Document you wish to export
2. Select File -> Download As
3. Select PDF
4. The document should start downloading

Once complete, you'll need to rename the file in accordance with your filenaming convention (unless of course you've been using this convention within Google Docs itself as well).