

Ogden City

What HAS and has NOT worked for us in making policies...

Records Management Ogden is on it's third system

Can you find all the data you need for your 'single view of the customer'?

At Ogden City, it is spread around through 8 departments, 22 divisions, several servers and various computer programs and software.

This includes three different citywide operating Records Management Systems.

The third time IS a charm!

- **Ogden City purchased a new records management system and has converted existing archives.**
- **Written policies and procedures are being documented with this system to ensure consistency and tracking.**
- **Includes policy items such as address and name format, and which documents are considered under which document type.**
- **Retention is defined for any record declared into the system.**

Other media types Ogden has yet to consider....

- **Individual PC electronic records or depositories**
- **Database records**
- **Telephone call recordings or other audio files**
- **Digital images**
- **Instant messages**
- **Video files**
- **Text messages**
- **Thumb drives**
- **Surveillance Tapes**
- **Others?**

We continue to ignore the elephants in the room...

Electronic records and E-mail.

- **Unbelievably, the 2007 Cohasset ARMA/AIIM Electronic Records Management Survey noted that more than 1/3 of organizations still do not include electronic records in their retention schedule.**
- **There has to be a way to gather e-mails under a centralized management umbrella so that those e-mails that need to be retained are kept and those deemed unnecessary are disposed of properly.**
- **We began our own pilot project by proceeding from the idea that solid records management principles are the foundation for addressing Ogden's e-mail concerns.**

E-mail as a liability...

- **Challenges around managing e-mail began in Ogden City with policy....or lack thereof.**
- **Since 2003, documentation shows that the Information Technology Division Manager, Records Manager and Legal Counsel had been meeting to attempt to create an e-mail policy.**
- **Each time, they reached a standstill because no one party could agree on policy.**
- **Meanwhile, E-Discovery is growing HUGE!**

E-Discovery Policy is Needed

How to determine when e-mail is a business record:

- An e-mail or an attachment is considered a business record if it contains information about the running of the business.**
- Keep privacy rules in mind.**
- An e-mail or attachment is usually considered a business record if it contains data about an employee or potential employee.**
- Can be viewed by regulatory agencies as an auditable source of company information to track how they do business.**
- Potential evidence in litigation.**

E-mail, a business record.

The average user sends 30 e-mails daily and receives over 100.

- My group felt an individual employee designated classification would be too time consuming.**
- Yet in contrast, they did not trust an automatic system.**
- There was no system in place to overrule deletions centrally for litigation holds.**
- Personal Storage (PST files) on individual computers were growing and there was no ability to manage or inventory content.**

PST's are evil...

- **They became popular because they are easy to use, provide a user with mobile access, and ease of storage management.**
- **Some PST files have been left unmanaged for over a decade.**
- **Individual review of PST files must be conducted and can prove to be an expensive nightmare for E-Discovery.**
- **They should be used for immediate access to information and not for any type of records storage.**
- **Is there a process in place to review and manage the files of former or departing employees?**

PST Legal Issues

- **There is no centralized management or search capability.**
- **All searching is manual.**
- **No retention or disposition compliance.**
- **No risk analysis.**
- **Lawyers have learned to target PST's because they prove to be an enormous risk to any organization, are easily transported, and sometimes are the only existing record of information.**

Most frequently stolen data

When employees leave, they take the following proprietary company data with them:

- **E-Mail lists** 65%
- **Non-financial business data** 45%
- **Customer contact lists** 39%
- **Employee records** 35%
- **Financial Data** 16%

Source: The Poneman Institute, 2009

Also, as you have more employees working from remote locations and on home computers, the concept of who really controls this data is not often clear to people.

E-mail – Retention Options

IT driven e-mail retention options:

- **Limit the size of the mailbox**
- **Purge after a define period**
- **Mailbox archiving (retention forever)**

E-mail archiving systems:

- **Allow for more efficient storage than native e-mail systems**
- **Allow more sophisticated retention, legal hold, and search of e-mail repositories**

We still need an adopted policy.

- **Write a project plan; document business processes.**
- **Determine what to do about data from employees that have left the company.**
- **Discover all existing PST's.**
- **Don't forget remote users.**
- **Store PST data in an archive to bring it under centralized management.**
- **This allows for setting proper retention, E-Discovery, risk management and early case assessment.**
- **Access for end users is very important.**

- **Think about when e-mail is created and sent; a copy of the e-mail exists on both the sending and receiving computer along with the servers that back up relative systems.**
- **Proper e-mail archiving is critical. With e-mail recognized as a business record, managing all e-mail information throughout its lifecycle is a management *must*.**
- **There is the need for capture of all e-mail data.**
- **Application of proper rules for retention and disposition.**
- **Facilitation of easy, comprehensive collaborative search and discovery of e-mail data.**

E-mail that must be saved (may not be deleted)

Program, policy or decision-making correspondence.

- **The sender and direct recipient of program, policy, or decision-making e-mail must retain the message.**
- **You are required to keep a copy of any attachments you send if they fall under the category of program, policy or decision-making correspondence.**
- **Primary responsibility for retention of important e-mail rests with the sender.**

E-mail that may be deleted.

All e-mail not falling into the above category may be deleted when the user's need for the e-mail has expires.

Examples of e-mail messages that do not need to be saved are:

- Personal e-mail**
- Routine correspondence**
- Meeting agendas, broad e-mail announcements and e-mails on which you are carbon copied and have no use for them.**

Any policy should be clear and supported by a written control document.

- **The controls should be tested and such tests documented.**
- **The system should have checks that can be monitored.**
- **Consider including the e-mail policy within the actual documentation retention policy for your organization.**
- **Consider policy that includes how to specifically wipe e-mail or electronic data from your systems.**

- **You need a tamper resistant archive and an automated system that enforces retention policies, including legal holds in the event of litigation.**
- **You need permanent removal of an e-mail from the archive at the expiration of the retention period.**
- **You need flexible retention management capabilities, including setting policies at various levels such as mailbox or folder.**
- **You need the ability to execute retention policies against message classes (e.g. voice-mail).**

Website Content & Records Management Mix

**A new website posting policy is introduced
in Ogden City.**

Ogden City unveiled it's new Website on April 9, 2009. Some exciting features included:

- **An eye-pleasing interface that changes with the seasons**
- **A search engine powered by google**
- **A new events calendar**
- **A searchable, step-driven document repository**

What did this mean to us?

- **In evaluating the existing Web site, it became obvious that the majority of the information was outdated and never removed from the website when its retention or timeliness had expired.**
- **It also became obvious there were many documents placed on the web that perhaps were not considered public documents and should not have been.**
- **Each individual department and many individuals had the ability to post their own items.**
- **Many items on the web were not contained in City archives.**

Along with the new website came a new policy for maintaining its content.

- Changes to existing content or a request to add new content must be made through the Recorder's Division.**
- I then review the Document Management system to determine if I have the record, if I should have the record, if I have the current version of the record, etc.**
- Content gathering is still an ongoing process and I never cease to be amazed at what goes onto the website that I did not have.**

Finally...when in doubt, just take the next small step.

The *bottom line* is that policies are necessary.

To become effective, they must be a directive from the top down.

- They must be simple, thought-out, and well-written for employees to understand.**
- Training must be offered.**
- Periodic review should be conducted.**
- Changes will be made.**
- Realize that resistance to change will occur.**