CenturyLink White Papers

Email Archiving, Compliance & eDiscovery for Legal Professionals
Email Archiving, Compliance & eDiscovery
Topic of Interest for Legal Professionals

The digital age is upon us and there is no doubt that businesses from all industries and sizes are relying on digital communications, particularly email, as one of the primary methods for communicating within their organization as well as externally with customers and partners. Large amounts of emails are being generated on a daily basis and will continue to grow into the foreseeable future.

This paper contains important information for any business or IT professional, but is particularly relevant for legal professionals as it applies to both best practices within their own firms but also in helping them advise their clients on strategy and tools they can use for the very important topics of Email Archiving, Compliance & eDiscovery.

Over the last 10 years, increased attention has been given to the topic of electronically stored information (ESI) as this type of data has become particularly important in the legal community as a means of providing evidence for certain types of litigation proceedings. In 2006, emails were explicitly named as likely records to be archived and produced when the U.S. Supreme Court amended the Federal Rules of Civil Procedure (FRCP) law. This means that when ordered to do so, businesses must be able to quickly produce all electronic content related to the case. It is pretty clear that every business faces some level of ESI regulation and compliance requirements whether engaged in a “heavily” regulated industry such as a broker-dealer or a “less heavily” regulated one common to most other industries.

It is important to all organizations, public or private, to develop an email archiving strategy that meets your internal compliance goals as well as any legal or industry requirements. Factors that organizations should be looking for in a solution include tamperproof read-only storage, multiple data centers, automatic quality verification, auditable message serialization, searchable data, attachments & metadata and transport & storage encryption. CenturyLink has SaaS solutions that can meet strict business and regulatory requirements in this area.

By Reading this White Paper you will learn:

• The importance of email archiving, compliance and eDiscovery.
• Regulations that can affect your business or that of your clients.
• The importance of establishing a successful program (best practices).
• How CenturyLink solutions can help.

eDiscovery – otherwise known as Electronic Discovery is the obligation of parties to a lawsuit to provide electronically stored information (ESI) such as emails upon court ordered requests. Under the Federal Rules of Civil Procedure (FRCP) now compel civil litigants to preserve and produce electronic evidence.
Email Archiving, Compliance & eDiscovery:
There are many reasons why an organization would benefit from using an email archiving solution such as complying with legal discovery and investigations, business continuity and disaster recovery, storage management and workplace compliance. Here is a closer examination of each of these categories to help you better understand this important topic.

Legal Discovery and Investigations:
We now live in a highly regulated world that requires companies to follow local, state and federal regulations. It is now expected and required that organizations be able to store and retrieve messages relevant to a legal proceeding when ordered to do so. As previously mentioned, recent amendments to the Federal Rules of Civil Procedure (FRCP) are now mandating emails as specific record types to be included for electronic discovery (eDiscovery). Outlined below are examples of the various regulations companies may be required to comply with.

Sample of Key Regulations:

FRCP: The Federal Rules of Civil Procedure (FRCP) are a set of guidelines set by the U.S. Supreme Court regulating court procedure for civil suits. FRCP often refers to revisions made in December of 2006 regarding electronic discovery, which became effective December 1, 2007. Electronic documents such as email, instant messages, or calendar files, and traditional documents stored electronically must be available for timely search and retrieval in the event of litigation proceedings. Discovery must be maintained in its original format. Accidental deletion, misplacement, or any inability to locate data before deadlines will result in court fines.

HIPAA: The Health Insurance Portability and Accountability Act was implemented by the United States Congress in 1996 to regulate health care providers’ management of protected health information (PHI), which includes medical records and payment histories. These regulations cover a broad range of administrative, technical and physical security measures. Regulated entities must maintain strict control over employees’ computer access to electronic PHI (E PHI) and ensure that historical EPHI is stored in a format with which no employee can tamper. IT should maintain written records of all configuration settings and changes. Audits should be performed routinely, along with documented risk analysis and risk management programs.

SEC 17a(3,4): A broker or dealer must preserve documents and records for three to six years, the first two years of which, they must be in an accessible place. All documents and records must be time-stamped, stored in a non-rewriteable/non-erasable format, organized and indexed, with a duplicate copy stored separately from the original. The indexes should also be duplicated and stored separately from the original, and they should be available for examination and preserved as long as the documents and records.

Sarbanes-Oxley Act: Requires public companies save all business records, including electronic records and messages, for not less than five years. In addition, public companies and registered public accounting firms must maintain audit work papers, documents that form the basis of an audit or review, and all information supporting conclusions for seven years. Given that, clearly email communications related to audit work papers and financial controls should be retained for at least seven years.

Investment Advisors Act: Investment advisers shall make and keep records in accordance with the Securities Exchange Act of 1934 as well as allow the Commission to examine such records as the Commission deems necessary or appropriate in the public interest or for the protection of investors. Investment advisers are also required to maintain and preserve books and records in an easily accessible location for at least five years from the end of the fiscal year during which the last entry was made, the first two years in an appropriate office of the investment advisers.

Source: MessageSolution – Compliance – Regulatory Overviews
http://www.messagesolution.com/resources.htm#frcp
Business Continuity and Disaster Recovery:
Given the importance and dependency of email communications within an organization, imagine how disruptive and costly it would be if there was a hardware failure that resulted in email data loss. This loss can be minimized by using a state-of-the-art, cloud-based solution that provides high-availability and redundant data centers as tools to achieve a secure Email Archiving, Compliance & eDiscovery solution.

Storage Management:
Email users and IT administrators are constantly trying to effectively manage the dreaded mailbox quota headaches. Besides offering legal and compliance solutions, email archiving can help control the costs and storage issues being faced by many organizations. Email messages can easily and seamlessly be offloaded from local company servers to secure SaaS email archiving solutions. Once emails are properly archived, older messages can be removed from local computers and servers.

Workplace Compliance:
Companies of all sizes share a similar risk when it comes to issues like discrimination, harassment, intellectual property management and possible loss/theft of proprietary corporate information. Email archiving solutions offer a level of protection against these risks by making it simple for company employees to automatically archive their emails and for administrators to search and retrieve required records. One example of how this can be applied is an administrator can search outbound messages that include proprietary information by using key word searches to help identify if there are any potential violations of the company’s information policies.

CenturyLink Email Archiving, Compliance & eDiscovery Solutions:
As a leader in SaaS and cloud-application solutions, CenturyLink has several products that can help businesses of all sizes implement and manage an email archiving and eDiscovery solution.

These cloud-based products offer a robust set of features that allow business users and IT administrators the tools necessary to deploy a cost-effective and easily implementable solution. Best of all, these are SaaS-based solutions, which mean no upfront capital outlay, no hardware or software to install or manage, and all are offered with affordable and flexible terms. Product features include:

- Archives all inbound, outbound and internal emails.
- Removes responsibility from end-users with automated policy application.
- Generates logs and reports.
- Reduces space by up to 60-80% on file servers for stored emails.
- Searches for emails and files including attachments from Web portal or client.
- Creates nearly unlimited mailbox space and eliminate email quota rules through continuous archiving.
- Increases IT productivity.
- Helps to improve compliance and litigation preparation.
- Simplifies tagging, notation and email analysis.
- Conducts high-speed forensic searches without the expense of outsourcing fees.
- Sets retention policy for one or multiple years.
As one of the premier benefits of purchasing an Email Archiving, Compliance & eDiscovery solution, customers can use CenturyLink’s FastForward Onboarding® that can help get you started with 24/7 CenturyLink support services.

Establish a Plan:
As a legal professional—whether helping your clients understand the importance of establishing a best practice approach to Email Archiving, Compliance & eDiscovery, or processes you need to put in place for your own firm— it’s critical to understand and outline needs and develop a plan. Here are some tips to help get you started:

• **Identify Regulatory Requirements**: Research what regulatory requirements your company is obligated to follow. These can be local, state or federal regulations. It is also important to understand what might be the recommended data retention practices for your particular industry. Analyze these requirements and initiate a plan based on a “High Watermark” approach.

• **Identify eDiscovery Scenarios**: As you are developing your email archiving plans it is important to remember to think about the types of eDiscovery requests you may have to respond to. These requests can come from inside or outside of your organization. Knowing what type of data would need to be recovered under different eDiscovery situations will help you to identify features you will need in your solution and what procedures you will need to put in place.

• **Establish Your Retention Policy**: There are a number of baseline recommendations for how long emails should be archived. Some suggest three years for educational related organizations and five years for corporations. The period of time you establish for email retention is only the beginning; establishing a well-documented policy is very important. Courts will look at the company’s policy to see if the entity has acted in “good faith” in applying its archiving and email deletion processes. Your policy should state the reason for your criteria and how your policy is to be followed. It goes without saying that adhering to the policy is paramount.

• **Involve all Stakeholders**: When developing your email archiving policy be sure that you involve all stakeholders in the organization such as legal, compliance, HR, finance, investor relations and IT. Your email archiving policy will affect every employee. So it is important to learn what kind of email and documents they use; how and when they refer back to older emails; and where they store their emails. This is just some of the information that will be important to learn from employees.

• **Socialize and Train Employees**: Make sure you develop processes and procedures that are easy for employees to understand and follow. It’s best to provide them with an understanding of how your email archiving policy is helping your organization comply with legal, regulatory or other types of requirements. Whenever practical, provide training on how to use the tools and technology. It is also recommended to refresh the training from time to time.

As a legal professional, it’s critical to understand and outline needs and develop a plan for your clients.
White Paper: Archiving, Compliance & eDiscovery

- **Eliminate PST Files**: If your organization is using Microsoft Outlook or Exchange then chances are users have created PST files on their local machines as a means of storing and accessing their older email files. However, it is important to make PST files read-only to minimize the legal risks that storing these files can have.

- **Shopping a Solution**: Armed with a plan for an Email Archiving, Compliance & eDiscovery process, now you can look for solutions that will meet your requirements. Critical to the success of your program is to find a solution this is as automated as possible for your end-users. Taking the burden off of them of having to manually perform email archiving tasks will ensure greater adoption and execution of your process. CenturyLink offers a number of cloud-based solutions that can meet even the most stringent of email archiving, compliance & eDiscovery needs.

Contact
Stay up to date on the latest CenturyLink news by reading our blog at centuryLink.com/blog. Or follow us on Twitter @CenturyLink, or like us on Facebook.

If you are interested in learning more about our SaaS-based Email Archiving, Compliance & eDiscovery, please visit us online at apps.centurylink.com, or call our Cloud Support Team at (855) 459-5121 today.