

Red Condor Hosted Archive Service

Meeting Compliance Requirements



Red Condor Archive provides an affordable, reliable and secure hosted Email Archiving Service to customers of all sizes to help you meet your compliance, litigation support, storage management or best practice requirements. Red Condor Archive leverages a global cloud computer and storage infrastructure to provide your organization with an extremely scalable, 100% software-free service, at an industry low price point. Red Condor Archive's data collection technology supports all messaging systems (Microsoft, Novell, IBM, Zimbra, Scalix, IMail Server, Mailtrust, Keiro and many more) making the solution truly future-proof.

Freedom Information Act "Sunshine Laws"

The federal government and nearly all state governments have established "Open Records" laws. The purpose of these laws is to provide a level of transparency to the activities of government agencies and officials to their citizens. There are no specific guidelines on how long emails must be retained. However, IT departments of these agencies must comply with the request for information which, in the absence of an email archiving solution, typically includes the laborious process of the restoration of backup tapes and the manual search across multiple mailboxes. In many cases, this search only produces a fraction of the emails pertaining to the request.

Red Condor Archive provides quick deployment of email archiving for all government agencies regardless of their email platform. With secure capture of all emails and full text indexing of emails/attachments, Freedom of Information requests are fulfilled with limited expenditure of IT resources.

Federal Rules of Civil Procedure (FRCP)

The U.S. Supreme Court ratified changes to the Federal Rules of Civil Procedure (FRCP), which took effect in 2006. These changes shift the rules of discovery in a legal proceeding from a focus on policies for electronic records retention, disposition and preservation, to a focus on procedures that will streamline evidence presentation.

Email and storage administrators must now answer key questions such as:

- * Where is the data in question?
- * What actions were taken to preserve it?
- * How can the data be searched and reproduced?
- * Just what is the company's established data retention/deletion policy?
- * Importance of METADATA

Red Condor Archive helps organizations comply with the Federal Rules of Civil Procedure as it pertains to email archiving by securely capturing, indexing and storing multiple copies of auditable email for easy retrieval through our search and discovery interface.

SEC 17A-4 and NASD 3010

The Securities Exchange Commission (SEC) originally enacted the Securities Exchange Act in 1934, as a means of protecting investors from fraudulent or misleading claims by securities dealers. The Act required member firms to create and maintain transaction records which could be reviewed and audited. In 1997, rule 17a-4 of the Act was amended to provide procedures for storage of electronic records, including emails. This rule has since been interpreted to include instant messages as well.

NASD (National Association of Securities Dealers) applies similar rules to its member firms through NASD 3010.

The provisions of SEC 17a-4 and NASD 3010 apply to all individuals and organizations involved in trading securities. This includes securities firms, stock brokerage firms, banks and any financial institutions that fall under SEC or NASD

Red Condor Hosted Archive Service

Meeting Compliance Requirements



jurisdiction. They require securities dealers to implement specific, enforceable retention procedures, which include the following:

Archived messages must be stored in duplicate. One copy must be stored in an online archive, and a second copy must be stored offline on permanent, tamperproof media, such as Write-Once-Read-Many (WORM) technology.

- Storage media must be verified automatically for quality and accuracy.

Red Condor Archive provides storage for all archived email on WORM compliant storage.

- Archived messages must be date/time-stamped and serialized. Each message must be assigned a unique, sequential identification number as a safeguard against deletion.

Red Condor Archive guarantees we capture messages with their original integrity in tact (Message ID, body, attachments, etc.) Messages are differentiated by a unique identifier as a safeguard against deletion.

- A searchable index of all stored data must be maintained. Indexes must be retained on each unit of storage media for the messages and attachments stored on that unit.

Red Condor Archive indexes all message components; Header, Body and Attachments and stores these securely.

- Messages and indexes must be easily retrievable and downloadable to other media as required by SEC regulators.

Red Condor Archive indexes all message components; Header, Body and Attachments. All of these components are easily searchable through a secure web based user interface and retrievable to standards based formats like .pst, .pdf, text, mime, etc.

SEC Investment Advisers Act of 1940

The U.S. Securities and Exchange Commission (SEC) has recently imposed new regulations on private investment pools, also known as hedge funds. The U.S. Securities and Exchange Commission, in a three-to-two vote on Oct. 26, 2005 decided to require hedge fund managers with assets in excess of \$25 million to register under the Investment Advisers Act of 1940. The regulation went into effect on Feb. 1, 2006. The ruling requires that most hedge fund advisers register with the SEC under the Investment Advisers Act of 1940, which includes provisions for securing, managing and archiving all electronic communication, including email and instant messages. **The rules governing the retention of electronic documents is the same as SEC 17 a-4.**

Sarbanes-Oxley (SOX)

The Sarbanes-Oxley Act of 2002 was enacted in the wake of several major corporate and accounting scandals. Its provisions affect email retention, integrity and oversight. Sarbanes-Oxley applies to all publicly traded companies and the CPA's and attorneys associated with these companies.

Section 802 presents a possible fine of up to \$1,000,000 dollars or a prison sentence of up to 20 years for any person who destroys, alters, mutilates or conceals any electronic document in an official investigation.

Sarbanes-Oxley specifies minimum retention periods for all accounting records, work papers, communications, file attachments, and documents whether transmitted via email, instant messaging or other message modes.

Section 302 requires CFO's and CEO's to personally certify and be accountable for their firms record retention policies and financial reports.

Section 404 requires auditors to certify the underlying controls and processes that are used to compile the financial results of a company. Email is a critical component in being able to achieve this certification.

Red Condor Hosted Archive Service

Meeting Compliance Requirements



Section 103(a) and 801(a) require companies to maintain all documents including electronic documents that form the basis of an audit or review for seven years.

Red Condor Archive assists companies in complying with the Sarbanes-Oxley Act as it pertains to email archiving by securely capturing, indexing and storing multiple copies of auditable email for easy retrieval through our search and discovery interface.

HIPAA

This law was passed in 1996 and took effect in 2001. All organizations and business which handle, maintain, store, or exchange private health or patient related-information, regardless of size, are subject to HIPAA. In addition to health care providers and insurers, this includes employers maintaining employee health records, life insurers, public health authorities, organ donation banks, pharmacies, long-term facilities, billing agencies and clearinghouses. Each instance of intentional unauthorized disclosure is punishable by fines up to \$250,000 and possibly 10 years of jail time.

Section 164.312 establishes safeguards for electronic storage and maintenance of individual health information. Organizations must ensure the confidentiality, integrity and availability of all protected electronic information it creates, receives or transmits.

Mandates the use of security measures in 164.312(e), like encryption, to protect electronic health information from unauthorized access while being transmitted over electronic networks.

In HIPAA section 164.312 the law establishes strict requirements regarding user access, authentication and data protection.

Section 164.308 requires covered entities to establish contingency plans for responding to emergencies which damage systems containing electronic protected health information. This includes the ability to maintain retrievable copies of electronic records and having disaster recovery plan to restore any loss of data.

Section 164.312(b) establishes audit controls to determine when messages were delivered, manipulated or when administrators accessed the system.

Red Condor Archive helps organizations comply with the HIPAA regulation as it pertains to email archiving by securely capturing, indexing and storing multiple encrypted copies of auditable email for easy retrieval through our search and discovery interface.

21 CFR Part 11 – Pharmaceutical Companies

This legislation was enacted by The Food and Drug Administration (FDA) in 1997 and enforced beginning in 2000. It governs the use of electronic signatures and electronic records by pharmaceutical manufacturing companies. It aims to insure that electronic media provide the same level of data integrity as the paper-based storage and retrieval systems they are increasingly replacing. It mandates that:

For electronic signatures to be considered the legal equivalent of handwritten signatures, they must be secure, unique and verifiable. Electronic signatures generally consist of a user name and password, which are tied to a specific computer.

For electronic records to be accepted by the FDA, they must provide an inclusive audit trail that is computer-generated, operator-independent, time-stamped and secure. The audit trail must preserve the total sequence of electronic events: record changes can not overwrite previous information. From the time a file is created, all additions, deletions and changes must be saved in such a way that they can be retrieved and reviewed at a later time,

Red Condor Hosted Archive Service

Meeting Compliance Requirements



and they must be traceable to the individuals who initiated them and who can be held responsible via their electronic signatures.

Red Condor Archive helps organizations comply with the 21 CFR Part 11 regulation as it pertains to email archiving by securely capturing, indexing and storing multiple copies of auditable email for easy retrieval through our search and discovery interface.

Gramm-Leach Bliley Act (GLBA)

The GLBA was signed in 1999 and became fully effective on July 1, 2001. The law applies to banks, brokerage firms, tax preparation companies, insurance companies, consumer credit reporting agencies and a wide variety of other financial services firms. Violations of the GLBA may result in a fine of up to \$100,000 dollars and 5 years in jail. The primary focus of the GLBA is the protection of customer's personal financial information.

Section 6801 - Regulated organizations must insure the security and confidentiality of customer records and information. In Section 6801 the law requires that access to all customer records be carefully controlled to prevent substantial harm or inconvenience to any customer.

Any storage location that contains sensitive customer information must be protected by strong access control and secure passwords.

In Section 6801 (b)(1) companies must ensure that email messages are kept secure and encrypted when being transmitted over a link.

Sensitive customer information must be protected in case of physical disaster or technological failure.

Red Condor Archive assists companies in complying with GLBA as it pertains to email archiving by securely capturing, indexing and storing multiple copies of auditable email for easy retrieval through our search and discovery interface.

Office of the Comptroller of the Currency Advisory Letter 2004-9

On June 14, 2004 the OCC Advisory sent out a letter highlighting issues regarding Electronic Record Keeping in light of the E-SIGN Act. 15 USC 7001. The purpose of this letter was to address key issues posed by electronic record keeping systems. The OCC Advisory letter stated that banks should implement an electronic record retention system to allow litigation, audits, bank supervision, and compliance with laws & regulations. Systems should also prevent external access by third parties, and provide back-up, internal controls, record destruction, and record retention.

Red Condor Archive assists companies in complying with OCC Advisory as it pertains to email archiving by securely capturing, indexing and storing multiple copies of auditable email for easy retrieval through our search and discovery interface.



888-9NO-SPAM
www.RedCondor.com