



Cryoserver

The Forensic Compliance System

Departmental Benefits

Cryoserver Ltd
14 Baden Place, Crosby Row
London, SE1 1YW
Tel: + 44 (0) 20 7251 1000
info@cryoserver.com
www.cryoserver.com



Novell.



Microsoft



Table of Contents

Cryoserver benefits all departments	3
1 Board of Directors	3
2 HR department	4
3 IT Department	5
4 Compliance Officers	6
5 Data Protection department	6
6 Legal department	7
7 Finance and Accounts department	8
8 Sales department	8
9 Employees	9

Cryoserver benefits all departments

No matter what department you are in, forensic compliance of email is an issue that you need to address. Cryoserver benefits all departments by limiting corporate liability, demonstrating good corporate governance and generating cost savings for the organisation (e.g. fulfil subject access requests quickly, reduce IT department workload). Cryoserver also benefits all employees by increasing privacy and confidentiality, ensuring that it is not possible to illicitly search through an employee's email.

Email and electronic document archives are corporate property, making the organisation responsible for the content and use of corporate email. Inadequate email management therefore can expose an organisation to enormous risks. Cryoserver can help limit that exposure by providing a technical solution for email management so that an organisation can demonstrate it took appropriate preventative steps by implementing an appropriate solution as defined under US, EU and UK legislation.

Failure to retain documents and records may result in court action against an organisation. Electronic documents and emails are admissible evidence in a court of law or employment tribunal. If installed at the highest forensic compliance level, Cryoserver will enable businesses to produce records with high evidential weight quickly and inexpensively, when needed.

Extensive and often conflicting regulations increasingly demand retention and fast retrieval of electronic documents (including emails) during mandated retention periods. By providing a complete record of all emails sent to, from and around your organisation, Cryoserver can produce the information demanded within seconds.

The following document illustrates how Cryoserver benefits all departments within an organisation.

1 Board of Directors

- Demonstrates full accountability and high standards of Corporate Governance to shareholders, employees and customers: Inadequate email management exposes an organisation to enormous risks and liabilities. Implementing Cryoserver demonstrates appropriate preventative steps to mitigate corporate liability
- Board members have personal liability if a corporate culture of racism or sexism is allowed to develop unchecked: Cryoserver acts as a deterrent once staff knows that an exhaustive record of all emails sent to, from or around the organisation is being kept

- Board members are held criminally responsible if child pornography is found either within the organisation's premises or its servers around the globe: Cryoserver retains and preserves the evidence until criminal prosecutions are complete, after which time a Trusted Third Party (TTP) such as KPMG's Forensic Accounting division will attend the Cryoserver and selectively delete the material in a forensically correct way and revalidate the Cryoserver
- Electronic documents (including email) are admissible evidence in a court of law or Employment Tribunal: If installed at the highest forensic compliance level, Cryoserver will enable businesses to produce information of high evidential quality quickly and cheaply, when needed
- By not allowing deletion, a Board member can 'prove a negative' by being able to prove that a particular email wasn't sent or received: This mitigates liability where matters of corporate governance may be at issue

2 HR department

- HR departments can carry out formal investigations without requiring IT departments to restore back-up tapes, in itself a breach of at least two parts of current Data Protection legislation
- Carry out very fast investigations, which also means false allegations can be immediately discounted
- Ensure greater employee privacy and prevents organisation-wide abuse by generating a fully encrypted audit trail every time an authorised search is conducted
- Comply with the long mandatory retention periods for employee records that stretch for many years after an employee may have left the organisation. Much of this data is sent via email - e.g. references, training records etc.
- Settle potential employment tribunal cases before going to court. By virtue of having a tamper-proof record of email correspondence, the full context of any accusations can be understood and assessed upfront
- Facilitates the monitoring of possible workplace harassment (e.g., racism, sexism, obscenity, porn, defamation, etc) by preserving a written and tamper-proof record of who said what to whom and when without expense of restoring back-up tapes

3 IT department

- No more email restorations on behalf of another department: Email restorations from back-up tapes take a disproportionate amount of time, are expensive to carry out, and often do not produce the evidence required. You can also import all legacy PST's and back-up tapes into Cryoserver as a one-off bulk import for fast searching
- Legal Compliance: It is a breach of Data Protection legislation for IT departments to search through email back-up tapes that may contain personal data and 'sensitive personal data' as defined by the Act. Tapes should only be used for disaster recovery purposes, NOT for any other purpose
- Centralised location for Personal Data: Users will use Cryoserver to find older emails instead of hoarding them on desktops because of mail quotas. It is a breach of Data Protection legislation and security directives such as BS 7799 to store sensitive data on PST files dotted around the organisation
- Exemption from criminal penalties: IT personnel have been prosecuted for carrying out orders from management to destroy electronic evidence. Data on Cryoservers in Data Centres cannot be destroyed or altered, thus removing IT personnel from deciding whether to carry out what may be a criminal act
- Eliminate restorations of individual emails for users: IT personnel can simply give the user a URL, then users can login with their existing network login (via LDAP, so zero maintenance for IT), access their own email records, and restore the email they need back to their inbox - all with zero training
- Save valuable mailserver storage space: Users learn to go to Cryoserver to search old email (usually because it's so much faster and offers advanced features) so IT mailserver admins can delete older mail on the servers much earlier, making mailservers run faster and needing less storage
- Real-time Replication: Cryoserver has RTR built in at the application level, which means messages can be sent to two or more Cryoservers at the same time, with full mirroring. This removes the danger of depending on a daily back-up which will only be able to restore data stored up to the point that the back-up was made
- Minimal staff training: The training to administer Cryoserver technical features (e.g. disk management) takes 10minutes, as does training for privileged users. Ordinary users simply use the URL you supply them, which requires zero training
- Minimal technical support: Cryoserver is a Forensic Compliance System; integrity is paramount. It is sealed with tamper-evident seals, so no maintenance from the IT department is required. The application can be

supported and upgraded remotely directly by Cryoserver, who have no access to the data

4 Compliance Officers

- Compliance with existing and current regulatory, legal and operational mandates in global jurisdictions
- Appropriate methods of capture and storage of data that meets both retention AND privacy legislative requirements
- Search email records in a variety of ways, such as date range, by user, by keywords, by random sample, by 'sounds like' words, by stemming etc, in order to comply with e.g. SEC regs.
- Ensures a complete record of all email correspondence by removing the ability to delete or alter emails
- Set a single retention period (suggested minimum seven years) to provide assurance that you will be able to produce ANY email records sent or received during this period
- Comply with short statutory discovery times (e.g. SEC 36hrs, FSA 24hrs, DPA 40 days, FoI 20 days etc.)
- Validates records by digitally fingerprinting the data at the instant of storage, and validated again when retrieved to prove that it is in the same state as when it was stored

5 Data Protection department

- Immediate compliance with your legal duty to protect personal data in email as required by the DPA. (How are you storing personal data in email? Is it secure? Encrypted? Or is it in plain text on a back-up tape?)
- Immediate compliance with your legal duty to limit access to personal data in email as required by the DPA. (Have you carried out a risk assessment specifically on email, and established who has access to those records?)
- Immediate compliance with your legal duty to audit access to personal data in email as required by the DPA. (Can you guarantee that no-one is able to access email records without leaving an audit trail a mile wide?)
- Put full controls around your management of personal data contained within emails

-
- Minimise the time and cost of processing Subject Access Requests (SARs) from the general public or disgruntled employees taking the company to an employment tribunal
 - Minimise the time and cost of processing Freedom of Information Act requests from the general public or media

6 Legal department

- Record employees making ad hoc contracts: these may legally obligate the company or incriminate the employee
- Create a forensically compliant record of email (including attachments) that can be used as admissible evidence in court
- Acts as a deterrent, prevents the likelihood of criminal activity on corporate premises when employees know their email activity is being captured. Also enables Legal Counsel to easily spot confidential documents leaving the business
- Facilitates the monitoring of possible workplace harassment (e.g., racism, sexism, obscenity, porn, defamation, etc.) by preserving a written and tamper-proof record of who said what to whom and when
- Provide the evidence needed to resolve any contract dispute: Contract actions are time-expired after six or more years after the date of breach, so organisations must keep everything - even when it's an ad hoc contract (e.g. "We'll get that to you by Friday")
- Contracts are very often altered, often unknowingly, by email. Again, retention for at least six years of all email is essential to be able to establish the facts
- Track and validate your own Intellectual Property: sending an email to yourself containing the company's latest IP provides an unalterable validated record of when that IP was created
- Refute false IP claims: Cryoserver can also be used to refute any false allegation e.g. claims such as "we emailed that IP to you three years ago and you've stolen it" can be immediately dismissed
- Cryoserver is particularly useful at law firms for speedy dispute resolution, where email is increasingly used by clients to give instructions, and used by lawyers to give advice to clients

7 Finance and Accounts department

- Cost savings: The cost of implementing a technical solution like Cryoserver is less than the cumulative costs of legal fees, fines and reputational damage. The savings in HR alone justify purchase, however there is also a very fast ROI in IT, Data Protection and Compliance departments
- Compliance with the 150+ different regulations and legislation covering records retention (e.g. Accounts departments are passing regulated data around in email; there is mandatory retention of business and accounting data for varying periods up to twelve years for the average limited company.)
- Compliance with cross-border and transatlantic financial regulations that now cover electronic data e.g. the Securities and Exchange Commission (SEC) requires that all financial organisations retain all documents for a minimum of five years; these documents must be easily accessible by the SEC within this period
- Spot confidential financial documents passing out of the company: Financial documents can be 'seeded' with keywords which Cryoserver will trap if emailed to anyone outside the company (even if the attachment name has been changed, or all the content has been pasted into another document)
- Due Diligence Data Freezing: The accounts department, by sending financial documents through the Cryoserver system, can demonstrate at any later date that the record could not have been altered in any way
- Save time and money by giving Cryoserver access to External Auditors: This can be as part of your Corporate Governance programme, or simply as a cost-saving measure

8 Sales department

- Sales Management can spot the organisation's sales database passing out of the organisation, and immediately detect any other illicit use of the messaging systems
- Sales Management can review an audit trail of contact with any customer from first contact to closing business. This helps with speedy dispute resolution regarding e.g. commission arrangements or promises made to clients
- Allows salespeople very fast access to customer or prospect information, or any other data that would be otherwise lost in old emails

- Quickly spot if employees are accidentally making ad hoc contracts - which may legally obligate the organisation or incriminate the employee e.g. "I'll have that for you by Tuesday" is a legally enforceable contract

Customer Service Department Benefits

- Customer dispute resolution: Customers (particularly members of the public) often come back many months after a transaction claiming that emails between customer and organisation made particular undertakings or promises e.g. "Yes, the room will have a sea view". The organisation can immediately call up a full list of all email traffic between customer and ANYONE at the organisation to determine what was agreed between the parties
- Irrefutable court evidence: The organisation can demonstrate, for example, that an email produced by the customer has been faked, or has been altered. The organisation can also prove a negative, in that it can demonstrate it DIDN'T send a particular email e.g. demonstrate it never sent an email saying "Yes, the room will have a sea view"

9 Employees

- Increased privacy: No-one can access the employee's email except as part of a formal investigation: It is not possible for others to casually read an employee's email, as access to the whole repository of data is restricted to named users carrying out a formal investigation
- The Data Guardian system provides a dual check on the security of personal data: Employees are assured that checks and balances are in place to prevent, for example, their boss snooping their email for no good reason
- Employee's rights under the Data Protection Act are protected by ensuring the data is kept physically secure, electronically secure via encryption, cannot be accessed except by named users, and an audit trail is kept.
- Comfort that an exhaustive, tamper-evident record of all email allows a true and complete picture of an employee's email usage should it ever be needed, e.g. a Court, or Employment Tribunal
- Fast searching of every email ever sent or received since the employee joined the organisation: Allows the individual employee to retrieve any accidentally deleted emails and immediately find knowledge hidden in old emails without having to resort to IT or cumbersome Exchange Search to fulfil this request
- Reassurance that you can finally prove a negative: The employee can prove that they DIDN'T send or receive a particular email. This is useful for speedy dispute resolution e.g. where a customer insists they sent an email in an attempt to gain compensation