

Regulatory Compliance

Since the mid-1990s, there have been a significant number of changes to the nature and content of information technology-related legal requirements. The complexity of today's compliance framework has left many businesses confused about what is required.

Terrorist attacks, accelerating globalization, high-profile corporate scandals and business-to-business Internet transactions have led to a dramatic rise in requirements to safeguard electronic customer and transaction data. In order to meet these requirements, organizations must design and implement comprehensive written information security policies.

The implications of non-compliance range from hefty fines to potential prosecution and imprisonment of senior executives. High profile cases, such as Enron are weighty reminders that compliance and regulation are serious business issues.

So, what do organizations need know to navigate the regulation matrix? More importantly, how can content security solutions help meet the compliance challenge?

The role of Content Security in Compliance

Complex and wide-ranging, regulatory compliance covers:

- Privacy
- Records retention and archiving
- Monitoring for compliance
- Recovery or discovery of information in response to litigation or court orders

From the Sarbanes-Oxley (SOX) Act to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), regulatory compliance requires vigilant content security policies for email,

including archiving and encryption.

SOX, for example, mandates that processes – including internal and external email – used to produce financial reports must be consistent, reliable, secure and accurate.

Organizations, therefore, need to ensure that email systems are spam and virus-free, and that internal and externally shared data is secure.

Without protection, the delivery or receipt of confidential data via email could be slowed down or even exposed through spam or a virus attack.

Protect, archive and retrieve

The SOX Act mandates that any email included in the documented financial reporting process is retained for seven years. The challenge is identifying the right emails to keep and finding them quickly and easily when required.

Many businesses estimate that more than 50 percent of emails are not required for compliance purposes. So how can organizations accurately store critical email?

How can Marshal help?

Marshal provides comprehensive secure email and Internet management solutions that integrate content filtering, compliance, secure messaging and archiving for businesses small and large. Marshal's flagship solutions, MailMarshal and WebMarshal, protect networks, business assets and employees from incoming, outgoing and internal email and Internet content threats.

Marshal's easy-to-use, modular and integrated content security management solutions are designed to:

- Assist businesses with regulatory, law and policy compliance (including policy enforcement)
- Secure IT assets and reputations
- Manage IT-related risks
- Control compliance-related legal exposure

Marshal's highly trusted MailMarshal SMTP and WebMarshal solutions can help organizations comply with local and international legal and regulatory requirements:

Threat protection

- MailMarshal SMTP provides protection at the Internet boundary against spam, viruses and other more direct attacks that can adversely affect email servers.
- MailMarshal's content security engine examines messages upon receipt and quarantines, redirects or marks them as necessary. This limits the spread of unsecured data both internally and externally.
- To stop malicious and reputation-damaging email from being sent or confidential information from being disclosed, MailMarshal's content security engine has outbound rules that examine messages for specific defined content before they leave the organization.



Regulatory Compliance

Privacy and non-disclosure policies

- MailMarshal's Lexical Analysis engine, TextCensor, allows businesses to automatically scan the text content of email either inbound or outbound, including attachments and web pages. Either use Marshal's default scripts or create custom criteria to block or restrict malicious content.

Retention requirements

- MailMarshal's email archiving abilities

Monitoring, archiving of email communications

- MailMarshal's reporting and archiving features
- MailMarshal either sits in front of an existing archiving solution or archives messages based upon specific business rules, recipient/sender addresses or upon key words or phrases. This provides the flexibility to archive all messages to or from certain groups or on certain subjects to reduce time and space used retaining unnecessary documents.

Secure transmission

- MailMarshal's support for encrypted email

Privacy and Security

- WebMarshal's ability to restrict webmail access and file uploads and downloads at http, https and ftp sites

Why Marshal?

Today, Marshal is the solution of choice for more than 18,000 organizations worldwide, protecting in excess of 7 million users.

- 10 years experience in total content security solutions
- Solutions for companies from 10 to 100,000+ users
- Global 24/7 support team
- TRACE team insights and updates
- More than 40% of the Global Fortune 500 companies rely on Marshal solutions for email and Internet security needs
- More than 60% of the European Fortune Top 50 Companies use Marshal
- 45% of the USA's Fortune Top 170 Companies use Marshal
- 40% of Asia's Fortune Top 50 Companies use Marshal



Marshal's Worldwide and EMEA HQ
Marshal Limited,
Renaissance 2200,
Basing View,
Basingstoke,
Hampshire RG21 4EQ
United Kingdom

Phone: +44 (0) 1256 848080
Fax: +44 (0) 1256 848060

Email: emea.sales@marshal.com

Americas
Marshal, Inc.
5909 Peachtree-Dunwoody Rd
Suite 770
Atlanta
GA 30328
USA

Phone: +1 404 564 5800
Fax: +1 404 564 5801

Email: americas.sales@marshal.com
info@marshal.com | www.marshal.com

Asia-Pacific
Marshal Software (NZ) Ltd
Suite 1, Level 1, Building C
Millennium Centre
600 Great South Road
Greenlane, Auckland
New Zealand

Phone: +64 9 984 5700
Fax: +64 9 984 5720

Email: apac.sales@marshal.com