

DISC IS THE SOLUTION FOR YOUR COMPLIANCE NEEDS

REAL WORLD PENALTIES

- ◆ **MERRILL LYNCH FINED \$150M**
– For improper use of internal Email communication
- ◆ **JP MORGAN FINED \$135M**
– For aiding Enron in its plot to disguise debt
- ◆ **CITIGROUP FINED \$120M**
– For aiding Enron in its plot to disguise debt
- ◆ **MORGAN STANLEY FINED \$27.5M**
– For mishandled email
- ◆ **BANK OF AMERICA SECURITIES FINED \$10M**
– For inability to reproduce email evidence for discovery
- ◆ **THE STATE BANK OF INDIA FINED \$7.5M**
– For failure to assure and monitor compliance with the Bank Secrecy Act
- ◆ **OPPENHEIMER & CO. FINED \$4.5M**
– Lacked adequate supervisory systems and controls
- ◆ **FOUR FIDELITY-AFFILIATED BROKER DEALERS FINED \$3.75M**
– For registration, supervision and email retention violations
- ◆ **SEC, NYSE, NASD FINE FIVE FIRMS TOTAL OF \$8.25M**
– For failure to preserve email communications
- ◆ **SECURITIES AMERICA FINED \$375,000**
– Over secret commissions directed to its broker

Financial firms are strictly governed by numerous regulations such as the Sarbanes Oxley Act, the Gramm-Leach-Bliley Act, the FRCP and others set forth by FINRA, the SEC and the FDIC. These regulations dictate how electronic information is to be handled and retained. Implementing comprehensive compliance systems can seem daunting, but it doesn't have to be. Digital Info Security Company™ (DISC), a one-stop shop for data compliance, simplifies the process by providing all of the IT solutions that your organization needs in order to avoid potential litigation and substantial fines for non-compliance.

Email Archiving for Compliance

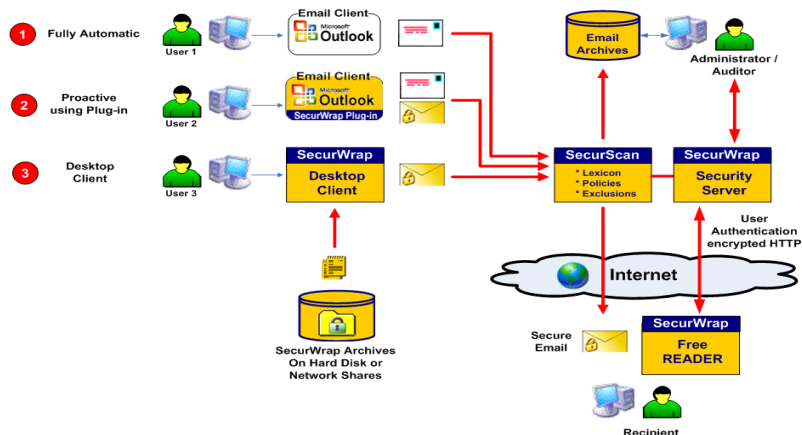
DISC's premier email compliance solution, PolicyBridge™ automatically archives and indexes all email and attachments while providing integrated email retrieval features. PolicyBridge™ supports industry standard storage solutions such as EMC Centera, StorageTek Libraries and all XFS compatible storage devices, including NAS, SAN, WORM, and optical. The integrated console allows for streamlined review of emails (pre/post process) and also provides a comprehensive set of archive retrieval tools for efficient discovery.

Email Surveillance & Active Policy Enforcement for Compliance

DISC's PolicyBridge™ scans email messages for sensitive, confidential, and proprietary information. In post-process mode, PolicyBridge™ flags the messages for review after they have left the mail server. In pre-process mode, PolicyBridge™ actively scans emails and enforces policies to block, quarantine, log or **encrypt** the flagged message.

Email Encryption for Compliance

DISC offers two methods of encryption for protecting private information. Using policy-based encryption, PolicyBridge™ can automatically encrypt messages that contain sensitive information as identified by the lexicon during customizable content scanning. This method eliminates human error and prevents data leaks. DISC also offers an email encryption plug-in, which encrypts a message from desktop-to-desktop using point-to-point encryption. This plug-in allows for digital rights management on secure email messages and works with multiple email clients. In order to meet data retention requirements, PolicyBridge™ also has the ability to archive all email messages and attachments. Additionally, PolicyBridge™ features extensive search capabilities for purposes of discovery and auditing.



Flash Drive and Removable Device Security

- ◊ **SecurFlash® Enterprise-** Enterprise encryption (AES 256 encryption) for USB Flash and Removable Drives. Portable and easy-to-use encryption and decryption with enterprise level administrative control for added protection.
 - ◆ **Highlighted features-** Detailed audit trail, revocation of lost drives, automatic user identity/password management, and easy to use drag-and-drop functionality.
- ◊ **SecurFlash® Administrator Server-** Command Center for Removable Drive Security. Comprehensive administrative control and policy enforcement for USB drives.
 - ◆ **Highlighted features-** Dynamically revoke access to lost or stolen devices, administrative audit trail, and ability to configure and enforce policies for out of network and offline use.



USB Device Control and Removable Drive Security

- ◊ **DeviceDefender™ Hosted Edition-** Affordable, transparent, and controllable detection management and encryption of USB port devices.
 - ◆ **Highlighted features-** Blocks unauthorized devices, provides automatic encryption of approved devices, supports all manufacturer devices and media, uses FIPS 140-2 certified encryption, and features the ability to revoke access to lost or stolen devices.
- ◊ **Administrator Server Edition-** Comprehensive administrative control and policy enforcement for removable drives and media.
 - ◆ **Highlighted features-** Administrative audit trail, ability to dynamically revoke access to lost or stolen devices, ability to configure and enforce policies for out of network and offline device use.



SecurServer

SecurServer provides consolidated user management, identity management and key exchange between senders and recipients of sensitive content. The SecurServer is a powerful tool that maintains a secure communication protocol with any sensitive data. It is controlled in a permission wrapper and provides a comprehensive audit trail on sensitive data in use throughout and outside of the enterprise. This audit trail includes user actions on the data, how that data has been shared, where it is located, and which users have access to it. Administrators may also revoke or expand user permissions directly from the Security Server console.

Data Retention for Compliance

RestoreRex® ensures that electronic records are protected against data loss and unauthorized access. Running automatically in the background, RestoreRex encrypts and backs up data on PCs and servers securely over the Internet to an offsite location.

Prevents Unauthorized Access – Only a designated administrator holds the encryption key to data.

Data Retention – Automatic backups preserve records offsite in an unalterable state. Regulations have varying retention requirements for up to seven years.

Secure Transmission – Data is encrypted while in transit over the Internet to DISC's data center.

