

# Complying with Data Security Standards

*Globalscape Solutions Help Companies Comply with a Variety of Security Mandates*

Complying with data security standards and industry regulations is vitally important in our interconnected world. Industry and government organizations have established numerous mandates intended to protect networks, the data transferred across them, and the people who are connected to the data. Just a few of the standards and regulations in the United States include the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes Oxley Act (SOX), IRS Publication 1075, and FIPS-140-2. In the United Kingdom, businesses and government offices are required to comply with guidance in the Data Protection Act (DPA), UK Code of Connection (CoCo), the Public Services Network (PSN), and ISO 27001.



Even though it takes a lot of effort to achieve and maintain compliance with these directives, complying with the standards applicable to your business can provide major benefits. For example, maintaining compliance can help you avoid fines and loss of business, shore up your corporate security plan, protect your reputation as a company that cares about security, and improve your IT structure overall. Meeting compliance standards in one security standard can also help you stay in compliance with all of the other regulations. Many businesses have an online or e-commerce component, and visitors to websites want assurance that their information, such as credit card numbers and personal data, is secure. Compliance with standards, certifications, and a history of data protection helps ease consumer concerns and encourages repeat business.

Customers and partners depend on businesses to keep their information secure. Following data security standards to bring your network into compliance is the best way to do that.

## Compromised Data Can Put You Out of Business

As we see quite often in the news, compromised data can have long-reaching negative effects for a business and its patrons. From industry and government fines to lawsuits, the financial costs are only one aspect—the damage to a business’s reputation might be irreversible. Failure to comply with mandates can have serious negative consequences to the business. One data breach can severely damage a company’s reputation and its ability to conduct business effectively, including loss of sales, damaged partner relationships, and lowered share prices for a publicly traded company.

In the case of the PCI DSS, credit card companies can refuse to accept charges by companies who do not comply with the standard. Each payment company also has their own security standards. For example, American Express requires compensation of up to \$100,000 for each data incident, plus card monitoring and replacement costs, and the card issuer's fraud chargebacks.

In the UK, before your organization can connect to the PSN, you must be accredited and achieve PSN compliance; you will either be assessed as compliant or rejected and unable to connect, and you must resubmit your application every year.

## Globalscape Solutions Facilitate Compliance with Security Mandates

The Enhanced File Transfer<sup>™</sup> (EFT<sup>™</sup>) managed file transfer solution with the High Security Module (HSM) achieves or exceeds security practices mandated by the most rigorous standards. Whether your business is obligated to comply or you simply want to establish and enforce the most rigorous security standards, the HSM is the solution for secure data transfer, access, and storage.

The HSM actively supports the PCI DSS and other standards by monitoring compliance, alerting administrators when non-compliance activity occurs, identifying the cause of non-compliance, allowing reverting of security controls, and implementing mitigation and workaround techniques. The HSM enforces strong account access controls such as the automatic lock out of accounts for users and administrators after a set amount of incorrect login attempts, and the automatic removal of inactive accounts. Additional security controls can be set to expire passwords automatically with custom email notifications. EFT's Auditing and Reporting Module (ARM) captures all of this activity in a relational database, and administrators can configure the automatic generation of reports for compliance auditors.

Securing sensitive company data requires continuous monitoring and validation of security policies and controls. Globalscape makes it easy for an administrator to create and maintain file-transfer services that meet or exceed these standards with a simple set-up wizard. For example, each page of the Site setup wizard describes a PCI DSS requirement and how to meet that requirement, and then allows the administrator to specify a compensating control (workaround). Once enabled, the HSM is an ever-vigilant security tool that disallows low-security options, captures compensating controls, and generates reports for auditing the system's compliance status.

Globalscape takes compliance seriously and follows all of the "best practices" mentioned in the PCI DSS and other standards, including considerations for customizations produced by our Professional Services team, use of common security frameworks, and development of our web client portals.

Globalscape's best-in-class MFT offerings feature robust data security that enables firms to meet and maintain all relevant compliance measures.