OPENTEXT™

OpenText Compliance Brief - PCI DSS

Overview of PCI DSS

Payment Card Industry Data Security Standards (PCI DSS) were developed in 2004 by four major credit card companies (Visa, MasterCard, Discover and American Express) as a collaborative effort to achieve a common set of security standards for the protection of credit cardholder data anywhere it resides within, or is transmitted by, a retailer's system. Its goal is to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information.

The PCI Data Security Standard is administered and managed by the PCI Security Standards Council (PCI SSC), an independent body that was created by the four payment card brands.

The PCI DSS specifies six main objectives:

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Non-compliance can result in fines, restrictions of credit card services and loss of consumer confidence. In addition to non-compliance fines, the PCI DSS allows the various payment card brands to fine a merchant for PCI non-compliance for each incident, as well as cardholder data compromised.

PCI DDS is now the de facto standard for measuring security programs for all merchants and service providers that participate in commerce using credit or debit cards.

INDUSTRY

Retail

WHO IS SUBJECT

All organizations or merchants, regardless of size or number of transactions, that accepts, transmits or stores any payment cardholder data

OPENTEXT™ SOLUTIONS

OPENTEXT™ PCI GATEWAY

***PCI Gateway** is a dedicated communication gateway built on OpenText's Information Exchange platform, which is certified by AT&T as PCI compliant. It removes credit card information and other sensitive data, and replaces it with secure tokens. Once the document has been tokenized, the rest of the flow is PCI compliant, that is, unless credit cards need to be de-tokenized at some point.*

OPENTEXT™ FAX2MAIL

OpenText maintains Level 1 Service Provider PCI Compliance for its Fax2Mail platform in Ashburn, VA. The platform is fully certified by a third party to transmit fax data featuring payment card information by adhering to the following security measures: data encryption in-transit and at rest, strict access controls around who is authorized to view data, immediate document deletion and no data archiving.

OPENTEXT™ IGC REDACT-IT ENTERPRISE

***IGC Redact-It Enterprise** is smart redaction software that protects people and business by removing sensitive information such as cardholder data from documents.*

Redact-It can perform batch redactions quickly with no scripting or complicated configuration. Or it can be integrated into OpenText Content Server or other enterprise content management systems to automatically remove sensitive content as an effortless part of your business process.

Redact-It completely removes redacted content from the output file so your enterprise can confidently move documents through the workflow process in a compliant manner.