

## PCI-DSS Compliance

The Payment Card Industry Data Security Standard (PCI-DSS) was adopted in 2004 by five major credit-card companies. Its purposes are to promote consistent global security standards and to protect cardholder data from fraud and security breaches. All merchants or service providers who store, process or transmit payment card account numbers are subject to PCI-DSS.

PCI-DSS is not just a technical concern. Its compliance mandates are also directed at "low-tech" positions, such as cashiers or anyone else who processes credit-card information. Even with all the right technical safeguards, human error or ignorance can be the cause of severe security lapses.

A security breach can affect the whole organization in profound ways — fines, loss of reputation or business, and even our ability to accept major payment cards, to name a few. This course instructs employees who handle payment-card information how to do so in accordance with PCI-DSS.

### Course Summary

This 40-minute course will explain the basic principles of PCI-DSS compliance and how they apply on the job. The topics covered in the course include —

- An overview of PCI-DSS
- PCI-DSS objectives and requirements
- Costs of non-compliance
- Sensitive Authentication Data
- Hard-copy storage
- Protecting cardholder information
- Payment-card transactions
- Remote access
- Good work practices
- Security incidents
- Restricted computer access
- Restricted physical access
- Tracking and monitoring
- Social engineering