



Lieberman Software

Maintaining Compliance with PCI Data Security Standards

The Payment Card Industry Data Security Standard (PCI DSS) was co-written by VISA and MasterCard, and endorsed by other leading credit card agencies, to establish measures for protecting its members against electronic fraud. It applies to all entities that store, process, or transmit cardholder account data, including retail merchants, payment processors, and banks. Failure to comply with PCI DSS policies can result in the creditor's loss of access to the crediting agency.

PCI DSS is divided into 12 requirements outlining different aspects of security best practices. These requirements include developing an information security policy, monitoring access to corporate networks, and implementing access control measures.

THE SOLUTION

Lieberman Software's privileged identity and security management solutions help secure and audit the use of highly sensitive information. These products address several facets of PCI DSS compliance regulations, such as changing vendor-supplied default passwords, assigning unique credentials to users, and tracking and monitoring access to important data.

PCI DSS OBJECTIVE	PCI DSS REQUIREMENT	LIEBERMAN SOFTWARE SOLUTION
Build and maintain a secure network	Requirement 2: Do not use vendor-supplied defaults for passwords	Automatically and frequently generate unique privileged account passwords
Protect cardholder data	Requirement 3: Protect stored data	Store current privileged passwords in encrypted database, with optional hardware-based encryption available
Maintain a vulnerability management program	Requirement 7: Restrict access to data by business need to know	Ensure that only delegated users can access privileged accounts
Implement strong access control measures	Requirement 8: Assign a unique ID to each person	Create unique administrator and root accounts so users are not sharing a common password
Implement strong access control measures	Requirement 8: Immediately revoke access for terminated users	Prevent former employees from being able to gain administrative access
Implement strong access control measures	Requirement 8: Implement two-factor authentication for user access	Ensure that only users with proper credentials and hardware token can access password store.
Regularly monitor and test networks	Requirement 10: Track and monitor all access to network resources and cardholder data	Produce audit-ready reports showing password changes and recoveries, and user access permissions
Maintain an information security policy	Requirement 10: Track and monitor all access to network resources and cardholder data	Produce audit-ready reports showing password changes and recoveries, and user access permissions