

The 6 Goals of PCI DSS versus Ocius Sentinel

Goal	PCI DSS Requirement	Ocius Sentinel aids by...
Goal 1: Build and Maintain a Secure Network.	Requirement 1: Install and maintain a firewall configuration to protect cardholder data.	
	Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.	Ocius Sentinel allows all user login and passwords to be managed via Commidea's secure online WebCom interface, through to its PCI certified data centres. This allows users to personally configure their own login and security details, even prior to installation. All Ocius Sentinel user validation data is stored as encrypted Hash values ensuring that security details are protected.
Goal 2: Protect Cardholder Data.	Requirement 3: Protect stored cardholder data.	Ocius Sentinel dual wraps the sensitive cardholder data on the PED. No decryption keys are held on site.
	Requirement 4: Encrypt transmission of cardholder data across open, public networks.	Prior to any cardholder data leaving the PED it is dual encrypted. This provides protection across any USB or RS232 connection from the PED and then across the local PoS network and beyond. This data is not unencrypted until it is safely within Commidea's PCI certified infrastructure.
Goal 3: Maintain a Vulnerability Management Program.	Requirement 5: Use and regularly update anti-virus software.	Ocius Sentinel's dual encryption of cardholder data prior to it reaching the PoS renders attacks from memory or traffic stealing malware ineffective.
	Requirement 6: Develop and maintain secure systems and applications.	Ocius Sentinel goes beyond PCI DSS requirements by using dual encryption and was the first solution to achieve PA-DSS certification.
Goal 4: Implement Strong Access Control Measures.	Requirement 7: Restrict access to cardholder data by business need-to-know.	Ocius Sentinel effectively removes cardholder data from the merchant's network whilst enabling the merchant to see full transaction history using Commidea's online WebCom reporting solution.
	Requirement 8: Assign a unique ID to each person with computer access.	Ocius Sentinel enables each operator to have unique access credentials.
	Requirement 9: Restrict physical access to cardholder data.	Ocius Sentinel dual encrypts the cardholder data within the PCI PTS certified device. A device specifically designed and certified to resist physical tampering. All other areas such as the PoS, which traditionally would have been vulnerable to physical tampering are protected via Ocius Sentinel's dual encryption.
Goal 5: Regularly Monitor and Test Networks.	Requirement 10: Track and monitor all access to network resources and cardholder data.	Ocius Sentinel records suspicious activities related to the PED and associated software. An audit trail can be obtained via Commidea's online WebCom interface.
	Requirement 11: Regularly test security systems and processes.	
Goal 6: Maintain an Information Security Policy.	Requirement 12: Maintain a policy that addresses information security.	Implementing Ocius Sentinel simplifies information security policy requirements as cardholder data is in one place only, the PCI PTS certified PED in the face-to-face environment.

*PCI compliance remains the responsibility of the retailer.

