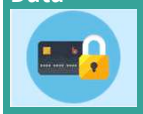
Fortytwo Security
Trusted in Information Security

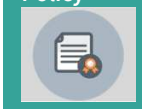
PCI DSS compliance checklist

Documents

Fortytwo Security BV
www.fortytwo.nl

SUBJECT	REQUIREMENTS	DOCUMENTS NEEDED	CHECK
Build and Maintain a Secure Network and Systems 	REQUIREMENT 1 Firewall and router configurations.	Firewall and router configuration	☐
		Network Diagram	☐
		Data Flow Diagram	☐
		Network Policy	☐
		Review Rule Set Process	☐
	REQUIREMENT 2 Document configuration parameters, and include the best PCI security practices.	Hardening configuration on all components in PCI scope	☐
		Inventory of system components	☐
Protect Cardholder Data 	REQUIREMENT 3 If disk encryption is used, how is access managed? Protect keys from disclosure and misuse to both data-encryption keys and key-encrypting keys.	Data Retention and Disposal policy	☐
		Data Retention and disposal Process	☐
		Disk Encryption Management	☐
		Key Management Policy	☐
		Key Management Process	☐
		Key Custodians Responsibility – Acceptance Form	☐
	REQUIREMENT 4 Documented standard showing strong cryptography and security protocols used to safeguard sensitive cardholder data during transmission over open, public networks.	Networking Policy	☐
		Hardening Configurations and/or Firewall and Router Configurations	☐
Maintain a Vulnerability Management Program 	REQUIREMENT 5 Vendor documentation regarding anti-virus programs capable of detecting, removing, and protecting against all known types of malicious software. Document and Implement an antivirus policy on all systems to ensure anti-malware protections.	Antivirus Policy	☐
	REQUIREMENT 6 Documented change control processes and procedures for all changes to system components. Document secure software-development procedures and policies.	Infrastructure Change Process	☐
		Software development Policy	☐
		Software development Process	☐
		Security Testing Process	☐
		Secure software development training	☐

Implement Strong Access Control Networks 	REQUIREMENT 7 Written access control policy, limiting access to system components and cardholder data. Policies and procedures for user identification management controls defined and in place for non-consumer users and administrators on all system component.	Access Control Policy	☐
	REQUIREMENT 8 Policies and procedures for user identification management controls defined and in place for non-consumer users and administrators on all system components.	Access Control Policy	☐
		Access Control Process	☐
		Roles and Responsibilities	☐
	REQUIREMENT 9 Observed, and documented facility controls to limit and monitor physical access to systems in the cardholder data environment.	Physical Access Policy	☐
		Physical Access Process	☐
		Physical Secure Storage Policy	☐
		Physical Secure Storage Process	☐
		Inventory of devices that capture payment card data process	☐
		Periodically inspect devices that capture payment card data process	☐
		Awareness training of attempted tapering or replacement of devices that capture payment card data	☐
Regularly Monitor and Test Network 	REQUIREMENT 10 Audit logs: for all system components within cardholder data environment. Examples: User ID, type of event, date and time, success or failure of indication.	System Monitoring Policy	☐
		System Monitoring Process	☐
	REQUIREMENT 11 Documented evidence of internal and external network vulnerability scans run at least quarterly and after any significant change in the environment. Documented evidence of internal and external Penetration testing run at least annually and after any significant change in the environment.	Wireless Scanning Process	☐
		Inventory of Authorized Wireless Access Points	☐
		Internal Network Vulnerability Scans	☐
		External Network Vulnerability scans (ASV)	☐
		External Penetration Testing	☐
		Internal Penetration Testing	☐

Maintain an Information Security Policy 	REQUIREMENT 12 Evidence of security policy established, published, maintained, and disseminated to all relevant personnel and service providers with whom cardholder data is shared.	Security Policy	☐
		Risk Assessment (at least annually and after significant changes)	☐
		Usage Policies	☐
		Security Awareness Program	☐
		Management Services Providers Process	☐
		Incident Response Plan	☐
		Roles and Responsibilities	☐
		HR Process	☐

This is our general list of documents that may be necessary for a PCI DSS audit. Depending on the implementation of the PCI environment and the type of business, this list can be modified. Contact us if you need help, info@fortytwo.nl or +31 20 4242320.