

PCI - Responsibility Matrix - FTD (Service Provider) / Florist

PCI DSS 4.0.1 Requirement 12.9

	REQUIREMENT 1	RESPONSIBILITY
1.1	Processes and mechanisms for installing and maintaining network security controls are defined and understood	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
1.2	Network security controls (NSCs) are configured and maintained	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
1.3	Network access to and from the cardholder data environment is restricted	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
1.4	Network connections between trusted and untrusted networks are controlled	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
1.5	Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
	REQUIREMENT 2	RESPONSIBILITY
2.1	Processes and mechanisms for applying secure configurations to all system components are defined and understood	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
2.2	System components are configured and managed securely	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
2.3	Wireless environments are configured and managed securely	<input type="checkbox"/> FTD <input checked="" type="checkbox"/> Florist <input type="checkbox"/> Joint
	REQUIREMENT 3	RESPONSIBILITY
3.1	Processes and mechanisms for protecting stored account data are defined and understood	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist

		<input type="checkbox"/> Joint
3.2	Storage of account data is kept to a minimum	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
3.3	Sensitive authentication data (SAD) is not stored after authorization	<input checked="" type="checkbox"/> Not Applicable
3.4	Access to displays of full PAN and ability to copy PAN is restricted	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
3.5	Primary account number (PAN) is secured wherever it is stored	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
3.6	Cryptographic keys used to protect stored account data are secured	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
3.7	Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
REQUIREMENT 4		RESPONSIBILITY
4.1	Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
4.2	PAN is protected with strong cryptography during transmission	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
REQUIREMENT 5		RESPONSIBILITY
5.1	Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood	<input type="checkbox"/> FTD <input type="checkbox"/> Florist <input checked="" type="checkbox"/> Joint
5.1.1	All security policies and operational procedures that are identified in Requirement 5 are: <ul style="list-style-type: none"> • Documented. • Kept up to date. 	<input type="checkbox"/> FTD <input type="checkbox"/> Florist <input checked="" type="checkbox"/> Joint

	<ul style="list-style-type: none"> • In use. • Known to all affected parties 	
5.2	Malicious software (malware) is prevented, or detected and addressed	<input type="checkbox"/> FTD <input type="checkbox"/> Florist <input checked="" type="checkbox"/> Joint
5.2.1	An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware	<input type="checkbox"/> FTD <input type="checkbox"/> Florist <input checked="" type="checkbox"/> Joint
5.2.2	<p>The deployed anti-malware solution(s):</p> <ul style="list-style-type: none"> • Detects all known types of malware. • Removes, blocks, or contains all known types of malware 	<input type="checkbox"/> FTD <input type="checkbox"/> Florist <input checked="" type="checkbox"/> Joint
5.2.3	<p>Any system components that are not at risk for malware are evaluated periodically to include the following:</p> <ul style="list-style-type: none"> • A documented list of all system components not at risk for malware. • Identification and evaluation of evolving malware threats for those system components. • Confirmation whether such system components continue to not require anti-malware protection. 	<input type="checkbox"/> FTD <input type="checkbox"/> Florist <input checked="" type="checkbox"/> Joint
5.3	Anti-malware mechanisms and processes are active, maintained, and monitored	<input type="checkbox"/> FTD <input type="checkbox"/> Florist <input checked="" type="checkbox"/> Joint
5.3.1	The anti-malware solution(s) is kept current via automatic updates.	<input type="checkbox"/> FTD <input type="checkbox"/> Florist <input checked="" type="checkbox"/> Joint

5.3.2	<p>The anti-malware solution(s):</p> <ul style="list-style-type: none"> Performs periodic scans and active or real-time scans. <p>OR</p> <ul style="list-style-type: none"> Performs continuous behavioral analysis of systems or processes 	<input type="checkbox"/> FTD <input type="checkbox"/> Florist <input checked="" type="checkbox"/> Joint
5.3.4	Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1	<input type="checkbox"/> FTD <input type="checkbox"/> Florist <input checked="" type="checkbox"/> Joint
5.3.5	Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period	<input type="checkbox"/> FTD <input type="checkbox"/> Florist <input checked="" type="checkbox"/> Joint
5.4	Anti-phishing mechanisms protect users against phishing attacks	<input type="checkbox"/> FTD <input type="checkbox"/> Florist <input checked="" type="checkbox"/> Joint
REQUIREMENT 6		RESPONSIBILITY
6.1	Processes and mechanisms for developing and maintaining secure systems and software are defined and understood	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
6.2	Bespoke and custom software are developed securely	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
6.3	Security vulnerabilities are identified and addressed	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
6.4	Public-facing web applications are protected against attacks	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
6.5	Changes to all system components are managed securely	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
REQUIREMENT 7		RESPONSIBILITY
7.1	Processes and mechanisms for restricting access to system components and cardholder data by business	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint

	need to know are defined and understood	
7.2	Access to system components and data is appropriately defined and assigned	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
7.3	Access to system components and data is managed via an access control system(s)	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
REQUIREMENT 8		RESPONSIBILITY
8.1	Processes and mechanisms for identifying users and authenticating access to system components are defined and understood	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
8.2	User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
8.3	Strong authentication for users and administrators is established and managed	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
8.4	Multi-factor authentication (MFA) is implemented to secure access into the CDE	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
8.5	Multi-factor authentication (MFA) systems are configured to prevent misuse	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
8.6	Use of application and system accounts and associated authentication factors is strictly managed	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
REQUIREMENT 9		RESPONSIBILITY
9.1	Processes and mechanisms for restricting physical access to cardholder data are defined and understood	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
9.2	Physical access controls manage entry into facilities and systems containing cardholder data	<input type="checkbox"/> FTD <input type="checkbox"/> Florist <input checked="" type="checkbox"/> Joint
9.2.1	Appropriate facility entry controls are in place to restrict physical access to systems in the CDE	<input type="checkbox"/> FTD <input type="checkbox"/> Florist <input checked="" type="checkbox"/> Joint

9.2.1.1	<p>Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows:</p> <ul style="list-style-type: none"> • Entry and exit points to/from sensitive areas within the CDE are monitored. • Monitoring devices or mechanisms are protected from tampering or disabling. • Collected data is reviewed and correlated with other entries. • Collected data is stored for at least three months, unless otherwise restricted by law 	<input type="checkbox"/> FTD <input type="checkbox"/> Florist <input checked="" type="checkbox"/> Joint
9.2.2	<p>Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility</p>	<input type="checkbox"/> FTD <input type="checkbox"/> Florist <input checked="" type="checkbox"/> Joint
9.2.3	<p>Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted</p>	<input type="checkbox"/> FTD <input type="checkbox"/> Florist <input checked="" type="checkbox"/> Joint
9.2.4	<p>Access to consoles in sensitive areas is restricted via locking when not in use</p>	<input type="checkbox"/> FTD <input type="checkbox"/> Florist <input checked="" type="checkbox"/> Joint
9.3	<p>Physical access for personnel and visitors is authorized and managed</p>	<input type="checkbox"/> FTD <input type="checkbox"/> Florist <input checked="" type="checkbox"/> Joint
9.3.1	<p>Procedures are implemented for authorizing and managing physical access of personnel to the CDE, including:</p> <ul style="list-style-type: none"> • Identifying personnel. • Managing changes to an individual's physical access requirements. • Revoking or terminating personnel identification. • Limiting access to the identification process or system to authorized personnel 	<input type="checkbox"/> FTD <input type="checkbox"/> Florist <input checked="" type="checkbox"/> Joint

9.3.1.1	Physical access to sensitive areas within the CDE for personnel is controlled as follows: <ul style="list-style-type: none"> • Access is authorized and based on individual job function. • Access is revoked immediately upon termination. • All physical access mechanisms, such as keys, access cards, etc., are returned or disabled upon termination 	<input type="checkbox"/> FTD <input type="checkbox"/> Florist <input checked="" type="checkbox"/> Joint
9.4	Media with cardholder data is securely stored, accessed, distributed, and destroyed	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
9.5	Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution	<input type="checkbox"/> FTD <input type="checkbox"/> Florist <input checked="" type="checkbox"/> Joint
9.5.1.3	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: <ul style="list-style-type: none"> • Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. • Procedures to ensure devices are not installed, replaced, or returned without verification. • Being aware of suspicious behavior around devices. • Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel 	<input type="checkbox"/> FTD <input type="checkbox"/> Florist <input checked="" type="checkbox"/> Joint
REQUIREMENT 10		RESPONSIBILITY
10.1	Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
10.2	Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint

10.3	Audit logs are protected from destruction and unauthorized modifications	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
10.4	Audit logs are reviewed to identify anomalies or suspicious activity	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
10.5	Audit log history is retained and available for analysis	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
10.6	Time-synchronization mechanisms support consistent time settings across all systems	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
10.7	Failures of critical security control systems are detected, reported, and responded to promptly	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
REQUIREMENT 11		RESPONSIBILITY
11.1	Processes and mechanisms for regularly testing security of systems and networks are defined and understood	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
11.2	Wireless access points are identified and monitored, and unauthorized wireless access points are addressed	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
11.3	External and internal vulnerabilities are regularly identified, prioritized, and addressed	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
11.4	External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
11.5	Network intrusions and unexpected file changes are detected and responded to	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
11.6	Unauthorized changes on payment pages are detected and responded to	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
REQUIREMENT 12		RESPONSIBILITY

12.1	A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
12.2	Acceptable use policies for end-user technologies are defined and implemented	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
12.3	Risks to the cardholder data environment are formally identified, evaluated, and managed	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
12.4	PCI DSS compliance is managed	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
12.5	PCI DSS scope is documented and validated	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
12.6	Security awareness education is an ongoing activity	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
12.7	Personnel are screened to reduce risks from insider threats	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
12.8	Risk to information assets associated with third-party service provider (TPSP) relationships is managed	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
12.9	Third-party service providers (TPSPs) support their customers' PCI DSS compliance	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint
12.10	Suspected and confirmed security incidents that could impact the CDE are responded to immediately	<input checked="" type="checkbox"/> FTD <input type="checkbox"/> Florist <input type="checkbox"/> Joint