Company Name or Logo

PCI Responsibility Matrix

PCI Requirement	<Company> Responsibility	Client Responsibility
1: Install and maintain a firewall configuration to protect cardholder data	Limiting network access to and from devices used within the <Company> online ordering platform to the most restrictive possible	Firewalls of all other networks controlled by <Company>'s client and other third parties chosen by the client.
Do not use vendor-supplied defaults for system passwords and other security parameters	Adhering to CIS-derived system hardening policies for all devices and systems within the <Company> online ordering platform.	Hardening of all other systems including in-store systems and third parties in PCI scope.
3: Protect stored cardholder data	Securely storing (or not storing) cardholder data within the <Company> platform in line with PCI Requirement 3.	Protecting cardholder data stored in-store or with non-<Company> providers
4: Encrypt transmission of cardholder data across open, public networks	Requiring secure transmission of cardholder data into the <Company> platform and sending data to payment gateways in the most secure manner supported.	Protecting in-store networks and all other third parties within PCI scope against malware
5: Protect all systems against malware and regularly update anti-virus software or programs	Regularly scanning <Company> platform servers for malware and viruses with up-to-date anti-virus software.	Protecting in-store networks and all other third parties within PCI scope against malware.
6: Develop and maintain secure systems and applications	Following secure development and change control procedures for all changes to <Company> platform components and ensuring that all <Company> platform components have the latest vendor-supplied security patches installed.	Ensuring that all non-<Company> platform and components follow secure development, change control and patching processes.
7: Restrict access to cardholder data by business	Restricting access to cardholder data to systems	Restricting access to cardholder data

need to know	and parties authorized by client.	transmitted or stored in-store and by all non-<Company> systems.
8: Identify and authenticate access to system components	Identifying and authenticating access to <Company> controlled components in PCI scope.	Identifying and authenticating access to non-<Company> components.
9: Restrict physical access to cardholder data	Restricting physical access to <Company>'s platform to PCI level 1 hosting providers.	Restricting physical access to all non-<Company>-controlled devices.
10: Track and monitor all access to network resources and cardholder data	Logging and monitoring all activity occurring within the <Company> Platform	Tracking and monitoring activity that occurs in-store and other non-<Company> systems within scope.
11: Regularly test security systems and processes.	Testing the security systems and processes for the <Company> platform	Testing non-<Company> security systems and processes within PCI scope.
12: Maintain a policy that addresses information security for all personnel		

Examples of <Company>’s Responsibilities

- Preventing credit card data from being intercepted in-transit between a client submitting credit card data and our platform servers.
- Preventing credit card data stored or transmitted within our platform from being stolen by unauthorized parties.
- Restricting access to sensitive data transmitted and stored by <Company>’s platform to only those with a business need.

Examples of Client Responsibilities

- Restricting traffic in and out of stores behind suitable firewall rules.
- Regularly updating operating systems and applications installed in-store
- Security of third party developers or agencies that develop on top of <Company>
- Security of POS system(s), payment processor(s) and loyalty service provider(s).

Examples of End-User Responsibilities

- Security of the device or browser being used to enter credit card data. For example, <Company> is not responsible for malicious browser plugins or key loggers.