PCI Responsibility Matrix

PCI Requirement	Olo Responsibility	Customer Responsibility
1: Install and maintain a firewall configuration to protect cardholder data	Limiting network access to and from devices used within the Olo online ordering platform to the most restrictive possible.	Firewalls of all other networks controlled by the customer and other third parties chosen by the customer.
2: 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 Olo 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 Olo platform in line with PCI Requirement 3.	Protecting cardholder data stored in-store or with non-Olo providers.
4: Encrypt transmission of cardholder data across open, public networks	Requiring secure transmission of cardholder data into the Olo platform, and sending data to payment gateways in the most secure manner supported.	Protecting cardholder data across all non-Olo networks falling within PCI scope, including the selected payment gateway.
5: Protect all systems against malware and regularly update anti-virus software or programs	Regularly scanning Olo platform servers in PCI scope for malware and viruses with up-to-date anti-virus software.	Protecting in-store networks and all other third parties within the PCI scope against malware.
6: Develop and maintain secure systems and apps	Following secure development and change control procedures for all changes to Olo components, and ensuring that all Olo components have the latest vendor-supplied security patches installed.	Ensuring that all non-Olo platform systems and components follow secure development, change control, and patching processes.
7: Restrict access to cardholder data by business need to know	Restricting access to cardholder data to systems and parties authorized by the brand.	Restricting access to cardholder data transmitted or stored in-store and by all non-Olo systems.
8: Identify and authenticate access to system components	Identifying and authenticating access to all Olo-controlled components in PCI scope.	Identifying and authenticating access to non-Olo components.
9: Restrict physical access to cardholder data	Restricting physical access to Olo's platform to PCI level 1 hosting providers.	Restricting physical access to all non-Olo-controlled devices

10: Track and monitor all access to network resources and cardholder data	Logging and monitoring all activity occurring within the Olo platform.	Tracking and monitoring activity that occurs in-store and other non-Olo systems within scope.
11: Regularly test security systems and processes	Testing the security systems and processes for the Olo platform	Testing non-Olo security systems and processes within PCI scope.
12: Maintain a policy that addresses information security for all personnel	Maintaining security policies for all Olo employees and contractors	Maintaining security policies for non-Olo personnel.

Examples of Olo’s Responsibilities

- Prevent credit card data from being intercepted in-transit between a customer submitting credit card data on Olo-hosted front-ends and our servers.
- Prevent credit card data stored or transmitted within our platform from being stolen by unauthorized parties.
- Restrict access to sensitive data transmitted and stored by Olo’s platform to only those with a business need.

Examples of Customer Responsibilities

- Restrict traffic in and out of stores behind suitable firewall rules.
- Regularly update operating systems and applications installed in-store.
- Secure third-party developers or agencies directed by the customer to develop to an Olo API.
- Secure POS system(s), payment processor(s), and loyalty service provider(s).

Examples of End-User Responsibilities

- Secure the device or browser being used to enter credit card data. For example, Olo is not responsible for malicious browser plugins or key loggers.
- Use strong, secure passwords