The Honest Company, Inc. Information Security Policy

Payment Card Industry Data Security Standard

Effective as October 26, 2022

Introduction

The Payment Card Industry Data Security Standard (PCI DSS) provides minimum requirements to maintain the security of cardholder data. PCI DSS applies to all card brands including Visa, MasterCard, Discover, JCB and American Express. Organizations that process, store or transmit credit card are subject to this standard. PCI DSS requirements change as there are new threats to payment card information and this policy will be updated periodically to reflect that.

The Honest Company collects credit card payments in a number of channels including eCommerce, Wholesale and Retail. There are required policies, processes, and technologies applicable to each environment.

PCI Policies

Card Holder Data

Payment card processing and data storage must be outsourced to a contracted PCI DSS compliant service provider and registered on VISA's Global Registry of Service Providers. PCI compliance status must be validated prior to onboarding a service provider that will manage, transmit, store cardholder data. All service providers that manage, transmit or store cardholder data must provide a current PCI DSS Attestation of Compliance (AOC) and are reviewed at least annually.

Card Holder Data Transmission

- Strong encryption algorithms and protocols (i.e., TLS, IPSEC, SSH) must be used whenever cardholder data is transmitted or received over open, public networks.
- Only trusted keys or certificates will be accepted The data transmission protocol must be implemented to use only secure protocol configurations and must not support insecure versions or configurations (e.g., use the latest secure TLS and SSH versions only). (PCI DSS Requirement 4.1.b)
- The encryption strength is appropriate for the encryption methodology in use. (PCI DSS Requirement 4.1.b) For TLS implementations, TLS must be enabled whenever cardholder data is transmitted or received. (PCI DSS Requirement 4.1.g) If SSL or early TLS is used on a POS POI terminal, documentation must be created detailing how it was verified that the terminal is not susceptible to any known exploits for SSL or early versions of TLS.
- Documentation must include evidence (vendor documentation, system /network configuration details, etc). (PCI DSS Requirement 4.1.h) If SSL or early TLS is used anywhere but a POS POI terminal, a risk mitigation and migration plan must be created, which includes the following: (PCI DSS Requirement 4.1.h) Access assigned to individual personnel is based on their job classification and function. (PCI DSS Requirement 7.1.3).
- An authorization form specifying all required access privileges is required and must be generated and signed by management approving the access. (PCI DSS Requirement 7.1.4)

Third-Party Service Provider Review

Careful consideration must be taken to evaluate third-party service providers hosting critical business that house and/or process restricted data, especially those within the scope of Sarbanes-Oxley and PCI, before

being on-boarded and annually to ensure they are secure, available, and operating accurately. Both technical and security assessments must be conducted prior to on boarding the service provider to determine compatibility with existing technical standards and compliance with security policies. Evidence of the most recent Disaster Recovery Plan and Testing along with SOC1 reports must be obtained and reviewed on an annual basis to identify any issues and verify alignment with existing Company security policies.

Employee Responsibilities

Employees must protect Company information and the information systems they use to process, store, or transmit Company information. Violations of these policies and standards or potential information security incidents must be reported to Management. Failure to comply with the IT Security policy may result in disciplinary actions up to and including termination of employment for employees or termination of contracts for third-party service providers.

Security Awareness Training

Annual information security awareness training must be provided to all employees and non-employees with access to non-public information. The information security awareness training must be based on The Honest Company’s IT Security policy and relevant legal and regulatory requirements.