PCI DSS Compliance Statement for Brandon Bridal Group, LLC D/B/A The Bridal Boutique on Tour

Effective Date: 06.01.2026

Last Updated: 06.01.2026

At Brandon Bridal Group, LLC, operating as The Bridal Boutique on Tour ("Company," "we," "us," or "our"), we are committed to ensuring the security of your payment information. This PCI DSS Compliance Statement outlines our adherence to the Payment Card Industry Data Security Standard (PCI DSS) v4.0.1 and our practices to protect your sensitive payment data. By using our website, https://www.thebridalboutiqueontour.com/ (the "Website"), you agree to the terms of this statement.

1. Commitment to Payment Security

We prioritize the security of your payment information and comply with PCI DSS v4.0.1 standards to safeguard cardholder data during every transaction. Our goal is to provide a secure shopping experience while protecting your sensitive information from unauthorized access or breaches.

2. Encryption and Security Measures

Data Encryption: All payment data transmitted through our Website is encrypted using Transport Layer Security (TLS) 1.2 or higher to ensure secure communication.

Tokenization: We utilize tokenization technology to replace sensitive cardholder data with unique tokens, reducing the risk of exposure during transactions.

Prohibition on Storing Sensitive Authentication Data: We do not store sensitive authentication data, such as CVV codes, PINs, or magnetic stripe data, after authorization, even if encrypted.

3. Compliance with PCI DSS v4.0.1 Standards

We adhere to the latest PCI DSS v4.0.1 standards, which include 12 core requirements for securing payment card data. These requirements cover areas such as maintaining secure networks, protecting cardholder data, implementing strong access controls, and regularly monitoring and testing networks.

4. Third-Party Payment Processor Information and Obligations

We partner with PCI DSS-compliant third-party payment processors to handle all payment transactions securely. These processors are responsible for storing, processing, and transmitting cardholder data on our behalf. We ensure that our partners meet all PCI DSS requirements and provide necessary certifications.

5. Customer Data Protection Practices

Data Minimization: We collect only the information necessary to process your transactions.

Prohibition on Storing Sensitive Data: We do not store sensitive authentication data, such as CVV codes or PINs, after authorization.

Access Controls: We restrict access to cardholder data to authorized personnel only, based on business needs.

6. Scope of Compliance

Our PCI DSS compliance applies to all systems and processes involved in storing, processing, or transmitting cardholder data. This includes our Website, third-party payment processors, and any other systems that interact with payment data.

7. Security Certifications and Validation

Self-Assessment Questionnaire (SAQ): As a Level 4 merchant, we complete the PCI DSS SAQ annually to validate our compliance.

Approved Scanning Vendor (ASV) Scans: We conduct regular vulnerability scans through an ASV to identify and address potential security risks.

8. E-Skimming Protection

We implement protections against e-skimming attacks in compliance with PCI DSS Requirements 6.4.3 and 11.6.1. These measures include: Monitoring and testing for unauthorized scripts or malware on our Website, and Ensuring secure development practices for all website updates and integrations.

9. Customer Responsibilities

To help us maintain a secure environment, we ask our customers to:

a. Use secure devices and networks when making purchases.
b. Report any suspicious activity or unauthorized transactions immediately.
c. Avoid sharing sensitive payment information via email or unsecured channels.

10. Contact Information for Security Concerns

If you have any questions or concerns about the security of your payment information, please contact us:

Email: brandonbridalgroup@gmail.com

Phone: ?

Address: ?

11. Placement on the Website

This PCI DSS Compliance Statement is accessible via the footer of our Website on every page. It is also available on our dedicated “Security and Compliance” page for your convenience.

12. PCI DSS Compliance Checklist

To ensure compliance with PCI DSS v4.0.1, we follow these best practices:

a. Build and Maintain a Secure Network:
    1. Install and maintain firewalls.
    2. Avoid using vendor-supplied defaults for passwords.
b. Protect Cardholder Data:
    1. Encrypt stored and transmitted cardholder data.
c. Maintain a Vulnerability Management Program:
    1. Regularly update antivirus software and secure systems.
d. Implement Strong Access Control Measures:
    1. Restrict access to cardholder data based on business needs.
    2. Use multi-factor authentication for access to sensitive systems.
e. Regularly Monitor and Test Networks:
    1. Conduct regular vulnerability scans and penetration testing.
f. Maintain an Information Security Policy:
    1. Train employees on security protocols and ensure compliance with PCI DSS standards.

By adhering to these practices, we aim to provide a secure and trustworthy shopping experience for all our customers. Thank you for choosing The Bridal Boutique on Tour for your special day.