Phorest PCI DSS Compliance Programme Overview

---

1. Purpose

This document provides an overview of Phorest's approach to payment security and PCI DSS compliance.

Phorest provides software and payment related services to customers across multiple markets. In doing so, Phorest works with approved payment service providers, including Stripe where applicable, to facilitate secure payment processing.

The purpose of this overview is to explain how Phorest approaches the protection of cardholder data, how Phorest works with Stripe and other payment service providers, and how Phorest manages its responsibilities under the Payment Card Industry Data Security Standard, known as PCI DSS.

This document is intended to provide customers and partners with a clear understanding of Phorest's payment security programme. It is not intended to replace formal PCI DSS assessment evidence, certification documentation, or contractual commitments.

---

2. Scope

This overview applies to Phorest Group companies, systems, products, and processes involved in, or capable of affecting, the security of payment card data or payment processing.

This may include, where applicable:

- Card present payments
- Online payments
- Online booking payments
- Payment links
- Card on file or stored payment method flows
- Deposits and prepayments
- Voucher and e-commerce payment flows
- Terminal integrations

- Payment service provider integrations
- Customer support processes relating to payments
- Internal systems used to administer, configure, support, or report on payment services.

The specific PCI DSS scope may differ by region, legal entity, product, payment flow, processor, and technical architecture. Each relevant payment environment is reviewed based on its role in storing, processing, transmitting, or potentially impacting the security of cardholder data.

---

3. Phorest's PCI DSS Compliance Approach

Phorest maintains a PCI DSS compliance programme appropriate to its role in the payment ecosystem and the payment services it provides.

Phorest's payment architecture is designed to minimise exposure to cardholder data. Where possible, Phorest relies on approved PCI DSS compliant payment service providers for the capture, processing, transmission, and storage of payment card data.

Where Phorest uses Stripe to facilitate payment processing, Phorest relies on Stripe's PCI DSS Level 1 Service Provider certification for the Stripe controlled elements of the payment processing environment.

Phorest remains responsible for the security and compliance of systems, applications, integrations, access controls, support processes, suppliers, personnel, and operational practices under Phorest's control.

---

4. Relationship with Stripe and Other Payment Service Providers

Phorest works with approved payment service providers to facilitate payment processing. Stripe is a key payment service provider used by Phorest in relevant markets and payment flows.

Stripe is certified as a PCI DSS Level 1 Service Provider. Phorest may rely on Stripe's compliance status for payment services, systems, and infrastructure controlled by Stripe.

Where Phorest uses Stripe hosted, Stripe controlled, or Stripe approved payment capture and processing flows, Phorest's exposure to cardholder data is reduced. However, Phorest must still ensure that its own systems, integrations, configurations, processes, and users are managed securely.

Phorest also seeks to maintain appropriate evidence of PCI DSS compliance from Stripe and any other relevant payment service providers, including attestations of compliance or equivalent documentation where applicable.

---

5. Shared Responsibility Model

PCI DSS compliance is a shared responsibility between Phorest, its payment service providers, customers where applicable, and any third parties involved in the payment environment.

Payment service providers, including Stripe where used, are responsible for maintaining PCI DSS compliance for the services and infrastructure they control.

Phorest is responsible for:

- Securely integrating with approved payment service providers
- Maintaining secure systems and applications under Phorest's control
- Limiting access to payment related systems
- Ensuring payment related changes are reviewed for PCI DSS impact
- Maintaining appropriate policies, procedures, and evidence
- Managing third party providers that may affect payment security
- Completing applicable PCI DSS validation activities
- Ensuring employees and contractors follow approved payment security procedures.

Use of a PCI DSS compliant payment provider helps reduce Phorest's PCI DSS scope but does not remove Phorest's own PCI DSS obligations.

---

6. Cardholder Data Handling

Phorest's approach is to minimise the collection, storage, processing, and transmission of cardholder data.

Where possible, cardholder data is captured, tokenised, processed, and stored by approved payment service providers rather than by Phorest systems.

Phorest does not knowingly store sensitive authentication data after authorisation, including:

- Full magnetic stripe data
- Card verification codes or values, including CVV, CVC, CID, or equivalent
- PINs or PIN blocks
- Unencrypted sensitive authentication data
- Any other data prohibited from storage under PCI DSS.

Where Phorest stores payment tokens, customer identifiers, transaction references, processor identifiers, or payment metadata, these are protected in accordance with Phorest security policies, data protection requirements, and applicable PCI DSS controls.

Employees, contractors, and support teams are required not to request, record, transmit, or store full card details outside approved payment flows.

---

7. PCI DSS Scope Management

Phorest reviews PCI DSS scope periodically and when material changes occur.

Material changes may include:

- Launch of a new payment product
- Launch in a new market or legal entity
- Change of payment service provider
- Change to terminal, online payment, or card on file architecture
- Introduction of new payment integrations
- Change to support processes involving payment data
- Change to infrastructure that may affect payment security
- Acquisition, restructuring, or migration of payment systems.

PCI DSS scope reviews may consider:

- Systems that store, process, transmit, or can impact cardholder data
- Third party service providers in scope
- Relevant legal entities and markets
- Applicable Self Assessment Questionnaire or assessment type
- Evidence required to support compliance
- Remediation actions required to address gaps.

---

8. Compliance Validation

Phorest maintains PCI DSS validation activities appropriate to its role and payment environment.

This may include, as applicable:

- Self Assessment Questionnaires
- Attestations of Compliance
- Service provider compliance evidence

- Penetration testing or vulnerability scanning evidence
- Security policies and procedures
- Network and system architecture documentation
- Supplier compliance records
- Internal control reviews
- External assessments where required.

The required validation may differ by entity, region, product, payment service provider, or payment flow.

Phorest's PCI DSS compliance programme is subject to review, and formal evidence may be provided where appropriate, subject to commercial, legal, confidentiality, and audit considerations.

---

9. Security Controls

Phorest maintains technical, organisational, and operational controls to support payment security and PCI DSS compliance.

9.1 Access Control

Access to payment related systems is restricted to authorised users with a legitimate business need.

Access is reviewed periodically and removed when no longer required.

9.2 Authentication

Administrative access to payment related systems is protected by strong authentication controls, including multi factor authentication where required.

9.3 Secure Development

Payment related software is designed, developed, tested, and deployed using secure development practices.

Changes to payment flows, payment integrations, or systems that may affect PCI DSS scope are assessed before release.

9.4 Vulnerability Management

Systems involved in or capable of affecting payment services are subject to appropriate vulnerability management, patching, monitoring, and testing.

9.5 Logging and Monitoring

Access to payment related systems is logged and monitored where appropriate.

Security events that may affect payment processing or cardholder data are investigated and escalated.

9.6 Data Protection

Payment related data is protected in accordance with PCI DSS, applicable data protection laws, contractual obligations, and Phorest security policies.

9.7 Supplier Management

Third parties involved in payment services or payment related support are reviewed for appropriate security and compliance standards.

Where a third party stores, processes, transmits, or can affect the security of cardholder data, Phorest seeks to obtain and review appropriate evidence of PCI DSS compliance.

---

10. Employee and Support Responsibilities

Employees and contractors are required to follow approved procedures when handling payment related matters.

Employees and contractors must not:

- Ask customers to provide full card details by email, chat, ticket, phone note, or any unapproved channel
- Record cardholder data in support systems, CRM systems, documents, spreadsheets, call notes, or messaging platforms
- Store sensitive authentication data
- Bypass approved payment flows
- Share payment system credentials
- Make unauthorised changes to payment configurations.

Any accidental receipt of cardholder data must be escalated and remediated in accordance with Phorest's security incident and data handling procedures.

---

11. Incident Management

Any suspected or confirmed compromise of cardholder data, payment systems, payment credentials, payment service provider integrations, or payment related infrastructure is escalated under Phorest's incident response process.

Where required, Phorest will notify relevant parties, which may include:

- Payment service providers
- Acquiring banks
- Card schemes
- Customers
- Regulators
- Law enforcement
- Affected individuals
- Other contractual or legal stakeholders.

Incident response activity is documented, investigated, and remediated.

---

12. Roles and Responsibilities

Executive Management

Executive Management is responsible for ensuring that PCI DSS obligations are understood, governed, and appropriately resourced.

Information Security / Compliance

Information Security or the relevant compliance function is responsible for maintaining the PCI DSS compliance programme, coordinating scope reviews, maintaining evidence, and advising on control requirements.

Product and Engineering

Product and Engineering teams are responsible for ensuring that payment products, integrations, and changes are designed and implemented securely.

Operations and Support

Operations and Support teams are responsible for following approved procedures when supporting payment related queries and must not request, record, or store cardholder data outside approved payment flows.

Commercial and Customer Facing Teams

Commercial and customer-facing teams are responsible for ensuring that payment related statements made to customers and partners are accurate, approved, and do not overstate Phorest's PCI DSS position.

Employees and Contractors

All employees and contractors are responsible for following Phorest's security policies and reporting suspected payment security issues immediately.

---

13. Customer and Partner Communications

Phorest seeks to provide customers and partners with clear, accurate information about its payment security approach.

Any external statement about Phorest's PCI DSS position should be accurate and limited to the relevant entity, product, region, payment flow, or assessment scope.

Phorest avoids broad or unsupported statements that could imply a wider certification or formal attestation than has been completed.

Preferred wording is:

"Phorest maintains a PCI DSS compliance programme appropriate to its role in the payment ecosystem and the payment services it provides."

Where a customer, partner, regulator, or supplier requires formal evidence, Phorest will review the request and provide appropriate documentation where available and permitted.

---

14. Current Programme Status

Phorest maintains an active PCI DSS compliance programme and continues to review its payment environments, supporting controls, third party dependencies, and validation requirements.

Where an audit, assessment, or formal validation activity is in progress, Phorest will treat the outcome as the authoritative evidence of its PCI DSS position once complete.

Until formal assessment evidence is finalised, this document should be understood as a customer facing overview of Phorest's PCI DSS compliance programme and payment security approach, rather than a formal certification, attestation, or guarantee of compliance.