PCI Compliance Documentation

Sandrake Solutions

Third-Party Service Provider Oversight Policy

(PCI DSS 12.8 compliance)

1 Purpose

This policy ensures that Sandrake Solutions maintains oversight of third-party service providers (TPSPs) that handle cardholder data on our behalf, even though our firm does not store, process, or transmit card data directly.

2 Scope

Applies to all payment activities processed through:

- Intuit/QuickBooks Online (invoicing and card payment processing)
- Venmo/PayPal (peer-to-peer and business transactions)
- Wells Fargo (Zelle, wire transfers, ACH)

3 Provider List

- Intuit/QuickBooks – Provides invoicing and card payment processing.
- Venmo/PayPal – Provides business payments and card acceptance.
- Wells Fargo (Zelle/wire/ACH) – Provides bank-to-bank transfers.

4 Written Agreements

Sandrake Solutions maintains Terms of Service / Merchant Agreements with each provider.

These agreements confirm that each provider is responsible for the security of cardholder data they process.

5 Due Diligence

Only established, PCI DSS–validated providers are selected.

Documentation of provider PCI compliance is reviewed annually (via their websites or compliance reports).

6 Responsibility Matrix

TPSPs: Responsible for all cardholder data processing, encryption, storage, and transmission.

Sandrake Solutions: Responsible for secure login credentials, enabling MFA, not downloading/storing raw card data, and training staff on secure practices.

Shared: Protecting access to accounts (passwords, MFA) and monitoring account activity.

7 Review

This policy and provider compliance status are reviewed annually and updated as needed.

Sandrake Solutions — Incident Response Plan

(PCI DSS 12.10 compliance)

01

Purpose

This plan defines how Sandrake Solutions will respond to suspected or confirmed payment security incidents that may affect our third-party payment accounts.

02

Scope

Applies to payment activities handled through Intuit/QuickBooks, Venmo/PayPal, and Wells Fargo.

03

Roles & Responsibilities

Incident Lead: James Sandlin

Contact: +1 (205) 534-4083 | james@sandrakesolutions.com

Responsible for initiating response, communicating with providers, and notifying clients if needed.

Incident Response Steps

1

Detection & Notification

If Intuit, Venmo, or Wells Fargo notify us of a potential breach or unusual activity, we act immediately.

2

Containment & Mitigation

Suspend payment activity until the issue is resolved.

Change account passwords, enable/verify MFA, and secure devices.

3

Communication

Contact affected clients if their payments may be impacted.

Follow provider instructions (Intuit, Venmo, Wells Fargo) for escalation and reporting.

4

Recovery

Resume normal operations only once the provider confirms systems are secure.

5

Documentation

Keep a written record of the incident, communications, and resolution steps.

Business Continuity

In case of prolonged outages, payments can be rerouted via Wells Fargo wire/ACH as backup.

Review & Testing

This plan is reviewed annually.

Updated immediately if payment methods or providers change.

Contact for Issues

James Sandlin – +1 (205) 534-4083 – james@sandrakesolutions.com