GRAND VALLEY STATE UNIVERSITY

Updated: March 2026

PCI DSS Responsibilities for Third-Party Service Providers

Grand Valley State University (GVSU) requires any Third-Party Service Provider (TPSP) that stores, processes, transmits, or could impact the security of payment card data to maintain current PCI DSS compliance and provide a valid Attestation of Compliance (AOC) upon request.

Vendors providing services that interact with payment card environments must demonstrate compliance with the Payment Card Industry Data Security Standard (PCI DSS) and acknowledge their responsibility to protect cardholder data.

Vendors claiming PCI DSS does not apply must provide documentation demonstrating that the services provided do not store, process, transmit, or impact the security of cardholder data or the cardholder data environment.

1. Scope of PCI DSS Compliance
PCI DSS applies to all entities that store, process, transmit, or can affect the security of cardholder data (CHD). This includes merchants, financial institutions, and Third-Party Service Providers (TPSPs).

Examples of TPSPs include:

- Hosting providers
- Online store or ticketing platforms
- Payment gateways
- Managed security service providers
- Cloud service providers

Even if a service provider does not directly store cardholder data, it may still be considered in scope if its services can impact the security of the Cardholder Data Environment (CDE).

2. Responsibility by Relationship

Organizations that use third-party vendors are required by PCI DSS (especially Requirement 12.8) to:

- Maintain a list of all service providers
- Ensure service providers are PCI DSS compliant

- Obtain a written agreement acknowledging the provider's responsibility for the security of cardholder data
- Monitor service providers' compliance status

Because of these requirements, GVSU must obtain documentation confirming vendor compliance.

Why an Attestation of Compliance (AOC) Is Required

1. Proof of Compliance

An AOC is a formal declaration by a service provider that they have undergone a PCI DSS assessment and are compliant. It provides:

- Evidence of assessment scope and validation method
- Description of services covered
- A summary of compliant and non-compliant requirements

Vendors must provide a current Attestation of Compliance (AOC) covering the services provided to GVSU. The AOC must clearly indicate that the services being provided fall within the validated PCI DSS assessment scope.

2. Transparency and Trust

Requiring an AOC:

- Ensures that security measures are not just assumed but independently verified
- Helps reduce organizational risk in the event of a breach
- Enables informed risk assessments and vendor selection

Failure to maintain PCI DSS compliance or provide an AOC may result in:

- Increased security and regulatory risk
- Inability for GVSU to validate PCI DSS compliance requirements
- Delays in vendor onboarding or payment processing integration
- Potential termination or suspension of services involving payment card data

Summary

Third-Party Service Providers that store, process, transmit, or can affect the security of cardholder data are subject to PCI DSS requirements.

GVSU requires vendors providing services to maintain current PCI DSS compliance and provide documentation such as a valid Attestation of Compliance (AOC).

These requirements help ensure the protection of payment card data and allow GVSU to meet its own PCI DSS obligations.

Please submit PCI DSS documentation or questions regarding these requirements to:
GVSU Information Security: security@gvsu.edu