

Elon University PCI DSS Compliance Addendum

Whereas Elon University secures services from _____ ("Service Provider") under an agreement ("Agreement") dated _____ (date), which services involve the processing of merchant card transactions, specifically _____; and

Whereas Elon University is required to adhere to the Payment Card Industry Data Security Standard (PCI DSS) promulgated by the PCI Security Standards Council; and

Whereas Service Provider processes, transmits, and/or stores cardholder data ("Covered Data") in the performance of services provided to Elon University, and is therefore considered a "service provider" under Requirement 12.8 of PCI DSS v4.0; and

Whereas Requirement 12.8.2 of PCI DSS v4.0 requires Elon University to maintain a written agreement with service providers that includes an acknowledgment that the service provider is responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of Elon University; and

Whereas Requirement 12.8.4 of PCI DSS v4.0 requires Elon University to maintain a program to monitor service provider PCI DSS compliance status at least annually;

It is hereby agreed that:

- 1) Service Provider agrees that it is responsible for the security of cardholder data that it possesses, including the functions relating to storing, processing, and transmitting of the cardholder data.
- 2) Service Provider affirms that, as of the effective date of this Addendum, it has complied with all applicable requirements of the then-current version of PCI DSS and has performed the necessary steps to validate its compliance.
- 3) Service Provider agrees to supply evidence of its current PCI DSS compliance status and most recent validation of compliance upon execution of this Addendum. Service Provider must supply updated evidence of compliance to Elon University at least annually thereafter.
- 4) Service Provider will immediately notify Elon University if it learns that it is no longer PCI DSS compliant and will immediately provide Elon University the steps being taken to remediate the non-compliance.
- 5) Service Provider acknowledges that it will indemnify Elon University for any failure of Service Provider to be and to remain PCI DSS compliant and for any failure of Service Provider to maintain the security of cardholder data that it possesses.
- 6) Service Provider will notify Elon University within twenty-four (24) hours of Service Provider's actual or reasonable knowledge of any breach of Elon University data.
- 7) Service Provider shall, upon termination, cancellation, expiration or other conclusion of the Agreement, securely destroy all instances of Covered Data in its possession,

including Covered Data held by subcontractors or agents of Service Provider. Service Provider shall complete such destruction within thirty (30) days of the conclusion of this Agreement and shall certify in writing to Elon University that destruction has been completed. Destruction includes all copies of the data, including backup copies created at any Service Provider or subcontractor site.

Elon University

By:

Name:

Title:

Date:

Service Provider

By:

Name:

Title:

Date:
